КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4
Побудова регістрів зсуву з лінійним зворотним зв'язком та дослідження їх властивостей

Мета роботи

Ознайомлення з принципами побудови регістрів зсуву з лінійним зворотним зв'язком; практичне освоєння їх програмної реалізації; дослідження властивостей лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.

Необхідні теоретичні відомості

2. Регістри зсуву з лінійним зворотним зв'язком

Лінійна рекурентна послідовність (ЛРП) порядку n *над полем* F_q – це послідовність (s_i), $i \geq 0$, що визначається за таким правилом:

1) початкові значення $s_0, s_1, ..., s_{n-1} \in F_q$ є довільними;

2) наступні значення обчислюються за формулою:

$$s_{i+n} = a_{n-1}s_{i+n-1} + a_{n-2}s_{i+n-2} + ... + a_1 s_{i+1} + a_0 s_i, \ \forall i \geq 0, \qquad (1)$$

де $a_t \in F_q$, $0 \leq t \leq n$-1– фіксовані коефіцієнти, а всі операції виконуються у полі F_q.

Формула (1) називається *лінійним рекурентним співвідношенням* для ЛРП.

Одержувати лінійні рекурентні послідовності на практиці можна за допомогою спеціальних апаратних пристроїв – *регістрів зсуву з лінійним зворотним зв'язком* (або просто *лінійних регістрів зсуву*, відповідна абревіатура ЛРЗ). Регістр зсуву описується схемою, наведеною на рис. 1.

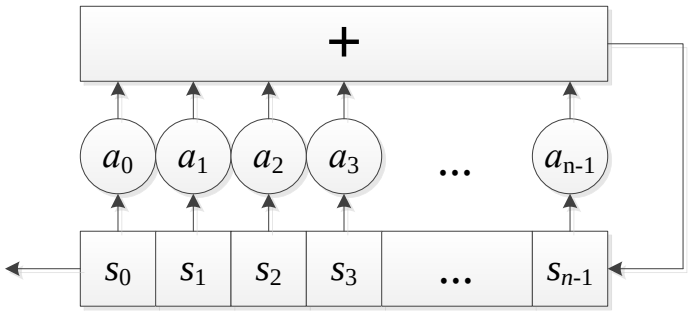

Рис 1. – Схема регістра зсуву з лінійним зворотним зв'язком

На кожному такті роботи регістр повертає значення нульової комірки на вихід, зсуває значення комірок на одну комірку в бік виходу, а в останню комірку заносить наступне обчислене за формулою (1) значення, яке відповідає наступному елементу рекурентної послідовності. Формула (1) є також *лінійним рекурентним співвідношенням* для відповідного ЛРЗ.

Станом регістра у деякий момент часу називається заповнення комірок у цей момент. Стан регістра природно розглядати як вектор над F_q. Зрозуміло, що послідовність, яку генерує регістр, повністю визначається коефіцієнтами зворотного зв'язку a_t, $0 \le t \le n-1$ та початковим станом регістру.

Властивості ЛРЗ та породжуваних ними лінійних рекурентних послідовностей добре вивчені. Так, лінійні рекурентні послідовності є періодичними. Дійсно, так як кількість різних станів ЛРЗ скінченна, то рано чи пізно деякий стан ЛРЗ повториться, а вся подальша послідовність залежить тільки від стану регістра у даний момент.

Якщо в деякий момент часу стан регістру стає нульовим вектором, то регістр надалі буде генерувати послідовність нулів. Таку послідовність вважають тривіальною, а цей випадок – небажаним. Втім, доведено, що якщо $a_0 \neq 0$, то послідовність, яку генерує регістр, буде суто періодичною (тобто не матиме передперіоду) за довільного початкового стану, і більш того, за цієї умови із ненульового стану регістр ніколи не потрапить у нульовий.

Властивості послідовностей, які генерує лінійний регістр зсуву, можна визначити аналітично за допомогою спеціального поліному, який називається *характеристичним поліномом ЛРЗ*; він також є *характеристичним поліномом* будь-якої *лінійної рекурентної послідовності*, що генерується даним регістром.

Порядком полінома $f(x)$ степеня n над F_q (позначається ord $f(x)$) називається найменше натуральне T таке, що $x^T - 1$ ділиться націло на $f(x)$; таке $T \le q^n - 1$ завжди існує. Якщо $f(x)$ незвідний над F_q, то ord $f(x)$ є дільником $q^n - 1$. Якщо ж при цьому ord $f(x) = q^n - 1$, тобто приймає найбільше значення, то поліном $f(x)$ називається *примітивним* поліномом степеня n над F_q (також примітивний поліном має бути нормованим, тобото мати старший коефіцієнт 1; ця умова не є обтяжливою, до того ж, як видно з наступної формули, для характеристичного полінома вона завжди виконується).

Для рекуренти, що описується співвідношенням (1), характеристичний поліном $p(x) \in F_q[x]$ має вид

$$p(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \ldots - a_1 x - a_0 .$$

За допомогою характеристичного полінома можна визначати періоди послідовностей, які генерує ЛРЗ, зокрема:

а) регістр генерує послідовності максимального періоду $q^n - 1$ тоді і тільки тоді, коли його характеристичний поліном є примітивним над F_q. У цьому випадку він пройде на протязі періоду через усі можливі ненульові стани;

б) якщо характеристичний поліном є незвідним над F_q, то послідовності, які генерує регістр при будь-якому ненульовому початковому стані, матимуть однаковий період, який співпадає із порядком полінома ord $p(x)$ над F_q; отже, період будь-якої ЛРП, згенерованої таким регістром ділить $q^n - 1$. Зворотне твердження не є вірним: за звідного характеристичного полінома можлива ситуація, коли всі ЛРП, згенеровані регістром, мають однаковий період, що ділить $q^n - 1$. Таким чином, якщо всі вихідні послідовності ЛРЗ мають однаковий період, то його характеристичний поліном *може бути* незвідним (і, скоріш за все, так і є);

в) якщо характеристичний поліном є звідним над F_q (тобто розкладається на нетривіальні множники), то довжина періоду, взагалі кажучи, залежить від початкового стану.

Відомо, однак, що послідовність максимального (серед усіх послідовностей, що генерує даний регістр) періоду задається початковим станом $\bar{d} = (0, 0, ..., 0, 1)$. Ця послідовність називається *імпульсною функцією.* У випадку звідного характеристичного полінома множина можливих періодів лінійних рекурентних послідовностей має складну будову, але існує теорія, що повністю її описує. Принаймні, якщо період імпульсної функції не ділить $q^n - 1$, то характеристичний поліном є звідним.

Отже, стани регістра, що змінюють один одного підчас його роботи, утворюють замкнені цикли. Кількість циклів та їх довжини (тобто періоди можливих послідовностей) будемо називати *цикловою структурою* множини послідовностей, що генерує регістр (або, коротше, цикловою структурою регістра). Послідовність $\boldsymbol{s}^t = s_t, s_{t+1}, s_{t+2}\ldots$ називають ***t-м зсувом*** послідовності ***s***. Очевидно, що усі зсуви даної послідовності належать одному й тому ж циклу. Якщо ЛРЗ генерує послідовності максимального періоду $q^n - 1$, то всі вони є зсувами одна одної і утворюють один цикл. Тому регістри з примітивними характеристичними поліномами називають *повноцикловими*.

Послідовності максимального періоду $q^n - 1$ виявились настільки важливими в теорії кодування, теорії обробки сигналів, задачах нелінійної локації та криптографії, що вони одержали окрему назву – *М-послідовності*. Серед іншого, доведено, що М-послідовності мають багато добрих статистичних властивостей, наприклад:

- всі символи зустрічаються у послідовності майже рівноімовірно, зокрема, у двійкових М-послідовностях кількість одиничок завжди на 1 більше за кількість нулів;
- всі *k*-грами, $k \le n$ розподілені на періоді настільки рівномірно, наскільки це можливо;
- функція автокореляції від послідовності приймає усього два значення (що свідчить про вкрай низьку залежність наступних символів від попередніх).

На практиці найчастіше розглядаються двійкові рекурентні послідовності, тобто лінійні рекуренти над F_2. Надалі ми будемо розглядати саме такі послідовності.

Функцією автокореляції зі зсувом *d*, $0 \le d < T$ періодичної двійкової послідовності $\boldsymbol{s} = (s_i)$, що має період *T*, називається функція $A_d(\mathbf{s}) = \sum_{i=0}^{T-1} [(s_i + s_{(i+d) \bmod T}) \bmod 2]$, тобто $A_d(\mathbf{s})$ - це кількість неспівпадаючих бітів на періоді послідовності ***s*** з циклічним зсувом того самого періоду на *d* позицій вперед.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Вибрати свій варіант завдання згідно зі списком. Варіанти завдань містяться у файлі Crypto_CP4 LFSR_Var.

2. За даними характеристичними многочленами $p_1(x)$, $p_2(x)$ скласти лінійні рекурентні співвідношення для ЛРЗ, що задаються цими характеристичними многочленами.

3. Написати програми роботи кожного з ЛРЗ L_1, L_2.

4. За допомогою цих програм згенерувати імпульсні функції для кожного з ЛРЗ і підрахувати їх періоди.

5. За отриманими результатами зробити висновки щодо влавстивостей кожного з характеристичних многочленів $p_1(x)$, $p_2(x)$: многочлен примітивний над F_2; не примітивний, але може бути незвідним; звідний.

6. Для кожної з двох імпульсних функцій обчислити розподіл k-грам на періоді, $k \le n_i$, де n_i - степінь полінома $f_i(x)$, i=1,2 а також значення функції автокореляції $A(d)$ для $0 \le d \le 10$. За результатами зробити висновки.

Оформлення звіту

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

- дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;
- для оформлення фрагментів текстів програм дозволяється використовувати шрифт Courier New 10pt та друкувати тексти в дві колонки;
- дозволяється не починати нові розділи з окремої сторінки.

До звіту можна не включати анотацію, перелік термінів та позначень та перелік використаних джерел. Також не обов'язково оформлювати зміст.

Звіт має містити:

- мету комп'ютерного практикуму;
- постановку задачі та варіант завдання;
- хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання;
- лінійні рекурентні співвідношення для ЛРЗ L_1, L_2;
- підраховані довжини періодів імпульсних функцій L_1, L_2;
- обчислені розподіли k-грам, $k \le n_i$, i=1,2 на періодах імпульсних функцій L_1, L_2;
- значення функцій автокореляції $A_d(\boldsymbol{s})$ для $0 \le d \le 10$, для відповідних імпульсних функцій;
- висновки щодо властивостей поліномів $p_1(x)$, $p_2(x)$ та вихідних послідовностей ЛРЗ L_1, L_2;
- відповіді на контрольні питання.

Тексти всіх програм здаються викладачеві в електронному вигляді для перевірки на плагіат. До захисту комп'ютерного практикуму допускаються тільки ті студенти, які оформили звіт та пройшли перевірку програмного коду.

Контрольні питання

1. Дайте означення лінійної рекурентної послідовності, лінійного регістра зсуву, імпульсної функції ЛРЗ.

2. Чим визначаються періоди послідовностей, які генерує ЛРЗ? За яких умов період набуває максимального значення?

3. Дайте означення порядку полінома степеня n над полем F_q та примітивного полінома степеня n над F_q.

4. Що таке M-послідовність, які її властивості?

5. Чому у двійкових M-послідовностях кількість одиничок завжди на 1 більше за кількість нулів?

6. Дайте означення функцій автокореляції $A_d(\boldsymbol{s})$ для двійкової послідовності $\boldsymbol{s}=(s_i)$, з періодом T.

7. Чи є сума двох лінійних рекурентних послідовностей (у двійковому випадку – XOR), згенерованих деяким ЛРЗ, також лінійною рекурентною послідовністю, що може бути згенерована тим самим ЛРЗ?

8. Які саме значення приймає функція автокореляції двійкової М-послідовності?

Оцінювання комп'ютерного практикуму

За виконання комп'ютерного практикуму студент може одержати до 9 рейтингових балів; зокрема, оцінюються такі позиції:

- реалізація програм – до трьох балів (в залежності від правильності та швидкодії);
- теоретичний захист роботи – до трьох балів;
- своєчасне виконання практикуму – 1 бал;
- несвоєчасне виконання роботи – (-1) бал за кожен тиждень пропуску.

Програмний код, створений під час виконання комп'ютерного практикуму, перевіряється на наявність неправомірних запозичень (плагіату) за допомогою сервісу *Stanford MOSS Antiplagiarism*. У разі виявлення в програмному коді неправомірних запозичень реалізація програм оцінюється у 0 балів, а за виконання практикуму студент одержує штраф (–10) балів.

Студенти допускаються до теоретичного захисту тільки за умови оформленого звіту з виконання практикуму та проходження перевірки програмного коду.