СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз

Мета роботи

Ознайомлення з деякими принципами побудови криптосистем на лінійних регістрах зсуву; практичне освоєння програмної реалізації лінійних регістрів зсуву (ЛРЗ); ознайомлення з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.

Необхідні теоретичні відомості

1. Статистичні критерії. Задача розрізнення гіпотез

Нехай для випадкової величини *X* її розподіл *P* невідомий або відомий частково. Тоді довільне твердження щодо *P* називають *статистичною гіпотезою*. Статистичні гіпотези поділяються на *прості*, які однозначно визначають розподіл *P*, та *складені*, які лише стверджують належність *P* до деякого сімейства розподілів.

Історично задачі визначення статистичних гіпотез формулюються таким чином: є деяка проста гіпотеза $H_0 : \{P = P_0\}$, яка стверджує, що розподіл випадкової величини *X* описується законом P_0, і чинність цієї гіпотези нам треба перевірити. Паралельно розглядається альтернативна (конкуруюча) гіпотеза H_1, яка може бути простою чи складеною. На основі спостережень та статистичних експериментів над *X* потрібно визначити, яка з двох гіпотез, H_0 чи H_1, має місце.

Статистичним критерієм називається деяке відображення з множини вибірок на множину гіпотез:

$$f : R^* \to \{H_0, H_1\}.$$

Неформально статистичний критерій можна визначити як строгу математичну процедуру, яка для кожної вибірки вказує найбільш адекватну гіпотезу про розподіл випадкової величини *X*, яка породила цю вибірку.

Ефективність статистичних критеріїв визначається такими параметрами, як похибки першого та другого роду. Ми називаємо *похибкою першого роду* (англ. *false rejection* або *false positive*) відкидання гіпотези H_0, коли вона є вірною, а *похибкою другого роду* (англ. *false acceptation* або *false negative*) прийняття гіпотези H_0, коли вона не має місця. Імовірності похибки першого роду α та похибки другого роду β визначаються відповідно:

$$\alpha = P(H_1 \mid H_0),$$
$$\beta = P(H_0 \mid H_1).$$

Чим вони менші, тим більш ефективним є статистичний критерій.

Загальна схема побудови статистичного критерію виглядає так:

1) Шукається деяка *статистика*, тобто функція від вибірки на множину значень *T*:

$$g : R^* \to T .$$

2) Виділяють так звану *критичну множину* $T_{кр} \subset T$ – множину таких значень *g*, сума імовірностей яких є дуже малою при вірній гіпотезі H_0.

3) Для спостережуваної вибірки $\hat{X} \in R^*$ обчислюється значення $g(\hat{X})$. Якщо $g(\hat{X}) \in T_{кр}$, то гіпотеза H_0 відкидається; якщо $g(\hat{X}) \notin T_{кр}$, то гіпотеза H_0 приймається.

В цій схемі просто визначається імовірність похибки першого роду: $\alpha = P(g(\hat{X}) \in T_{кр})$.

Опишемо окремий клас статистичних задач, так звані *задачі розрізнення гіпотез*. В цьому випадку обидві гіпотези, H_0 та H_1, є простими, тобто стверджується, що випадкова величина *X* може мати лише один з двох даних фіксованих розподілів, і на основі спостережень за її реалізаціями треба встановити, який саме. Зрозуміло, що така постановка задачі набагато простіша, аніж у загальному випадку.

Покажемо схему побудови статистичного критерію, якій розв'язує задачу розрізнення гіпотез, на такому прикладі. Нехай випадкова величина *X* підкорюється нормальному розподілу, причому якщо вірна гіпотеза H_0, то параметрами розподілу є $a = 5$, $\sigma^2 = 4$, а якщо вірна гіпотеза H_1, то параметрами є $a = 10$, $\sigma^2 = 8$. Будемо розглядати вибірки з однієї реалізації та покладемо $g(\hat{X}) = \hat{X}$ (тобто статистикою є обчислене значення реалізації *X*). Тоді, зрозуміло, якщо $\hat{X}$ ближче до 5, то вірною треба обрати гіпотезу H_0, а якщо до 10, то гіпотезу H_1. Щоб формалізувати процедуру, оберемо деяке порогове значення $C \in [5, 10]$ та визначимо критичну множину $T_{кр} = \{X : X > C\}$. Очевидно, що саме вибір порогу визначає імовірності похибок першого та другого роду, причому ці значення пов'язані між собою: зменшення α (тобто зсув *C* вліво) призводить до збільшення β та навпаки.

2. Регістри зсуву з лінійним зворотним зв'язком

Лінійна рекурентна послідовність 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 $a_t \in F_q$ – фіксовані коефіцієнти, а всі операції виконуються у полі F_q.

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.

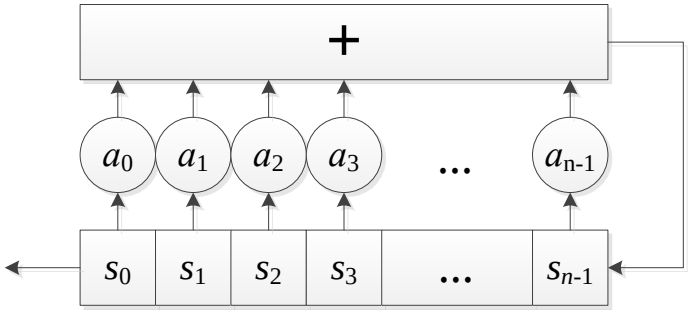

Рис 1. – Схема регістра зсуву з лінійним зворотним зв'язком

На кожному такті роботи регістр повертає значення нульової комірки на вихід, зсуває значення комірок, а в останню комірку заносить наступне обчислене значення, яке відповідає наступному елементу рекурентної послідовності.

Станом регістру називається заповнення комірок у деякий момент часу. Стан регістру природно розглядати як вектор над F_q. Зрозуміло, що послідовність, яку генерує регістр, повністю визначається коефіцієнтами зворотного зв'язку a_i та початковим станом регістру.

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 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 $f(x)$ над F_q (позначається ord $f(x)$) називається найменше натуральне T таке, що $x^T - 1$ ділиться націло на $f(x)$; таке $T \leq q^n - 1$ 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.

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 поліному можна визначати періоди послідовностей, які генерує ЛРЗ, зокрема:

а) якщо характеристичний поліном є незвідним над F_q, то послідовність, яку генерує регістр при будь-якому ненульовому початковому стані, матиме однаковий період, який співпадає із порядком полінома ord $p(x)$ над F_q;

б) Якщо характеристичний поліном є примітивним над F_q, то регістр буде генерувати послідовність максимального періоду $q^n - 1$, і в процесі генерування він пройде через усі можливі ненульові стани;

в) якщо характеристичний поліном розкладається на нетривіальні множники над F_q, то поведінка періоду починає залежати від значення стану. Відомо, однак, що в цьому випадку послідовність максимального можливого періоду задається так званою *імпульсною функцією* – початковим станом $\bar{d} = (0, 0, ..., 0, 1)$.

Послідовності максимального періоду 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 якісних статистичних властивостей, наприклад:

- всі символи зустрічаються у послідовності майже рівноімовірно;
- всі *k*-грами розподілені у періоді настільки рівномірно, наскільки це можливо;
- функція автокореляції від послідовності приймає усього два значення (що свідчить про вкрай низьку залежність наступних символів від попередніх).

В задачах криптографії найчастіше розглядаються двійкові рекурентні послідовності, тобто лінійні рекуренти над F_2. Втім, безпосереднє використання таких послідовностей, наприклад, в якості ключів є ненадійним через виключно лінійні залежності. Тому існує декілька способів внесення нелінійності у роботу регістрів та генерування відповідних послідовностей.

1) *Схеми нелінійної фільтрації*: на кожному такті деяка нелінійна булева функція застосовується до стану регістра (або тільки до його окремих біт). Значення функції є бітом вихідної послідовності.

2) *Схеми нелінійної комбінації*: використовується декілька ЛРЗ, виходи яких подаються на вхід деякої нелінійної булевої функції. Значення функції є бітом вихідної послідовності.

3) *Схеми нелінійного зворотного зв'язку*: у регістрі лінійна рекурентна залежність (1) замінюється на нелінійну. Поведінка регістру при цьому стає вкрай непередбачуваною. Вихід регістру є бітом вихідної послідовності.

4) *Схеми із нерівномірним рухом*: регістр працює нерівномірно, виконуючи за один крок декілька тактів (зсувів). При цьому поведінка регістру зазвичай задається іншим регістром, який називається *керуючим*. На цьому принципі побудовані так звані *stop-and-go*-генератори та (*i, j*)-*steps*-генератори.

5) *Стискаючі генератори*: послідовність, яку генерує лінійний регістр, або яка знімається із бітів його внутрішнього стану, перетворюється на нову послідовність визначеними правилами заміни. Наприклад, у ABC-генераторі, який використовується у потоковому шифрі DECIM^{v2}, фрагменти вхідної послідовності виду 00 та 10…01 замінюються на біт 1, а фрагменти 11 та 01…10 – на біт 0.

3. Генератор Джиффі

Генератор Джиффі (Geffe) є прикладом криптосхеми, побудованій на основі нелінійної комбінації ЛРЗ. Схема генератора Джиффі наведена на рис. 2, де через L_1, L_2, L_3 позначені ЛРЗ, що генерують відповідно двійкові послідовності (x_i), (y_i), (s_i), $i = 0, 1, 2, ...$ Знаки вихідної послідовності (z_i) обчислюються як $z_i = F(x_i, y_i, s_i)$, де

$$F(x, y, s) = sx \oplus (1 \oplus s)y, \qquad (2)$$

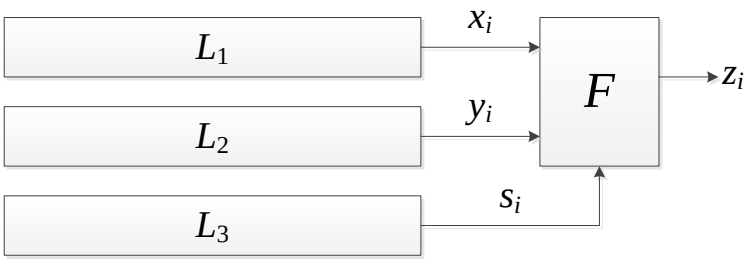

Рис. 2 – Схема генератора Джиффі

З (2) випливає, що регістр L_3 є керуючим у схемі генерації: при $s_i = 1$ на вихід схеми подається x_i, при $s_i = 0$ подається y_i. Ключем криптосхеми є початкове заповнення всіх трьох регістрів L_1, L_2, L_3.

Передбачається, що ЛРЗ L_1, L_2, L_3 генерують послідовності максимального періоду, тобто їх характеристичні многочлени – примітивні. Таким чином, послідовності (x_i), (y_i), (s_i) мають добрі статистичні властивості та їх можна розглядати як чисто випадкові, тобто послідовності незалежних рівномірно розподілених випадкових величин.

4. Криптоаналіз генератора Джиффі

Генератор Джиффі має суттєвий недолік: інформація про послідовності окремих регістрів «витікає» в гаму, яка генерується, і може бути використана аналітиком для пошуку початкових станів (які й є ключем шифрування). Дійсно, оцінимо імовірність того, що вихідний біт співпадає із бітом, який був згенерований першим регістром. Маємо:

$$\Pr\{F(x,y,s)=x\} = \Pr\{sx \oplus (1 \oplus s)y = x\} = \Pr\{s=0\}\Pr\{y=x\} + \Pr\{s=1\} = \frac{3}{4}. \qquad (3)$$

Аналогічно $\Pr\{F(x,y,s)=y\} = \frac{3}{4}$. Отже, функції $F_1(x,y,s)=x$ та $F_2(x,y,s)=y$ є *статистичними аналогами* функції $F(x,y,s)$, тобто такими функціями, що співпадають з $F(x,y,s)$ із імовірністю, суттєво відмінною від 1/2. Це означає, що вихід схеми корельований з виходами ЛРЗ L_1 та L_2; цю обставину можна використати для криптоаналізу схеми.

Нехай відомі *N* знаків послідовності (z_i) на виході генератора Джиффі: $z_0,\ldots,z_{N-1}$. Потрібно знайти ключ. Позначимо довжини ЛРЗ L_1, L_2, L_3 через n_1, n_2, n_3. Випробуємо спочатку всі можливі початкові заповнення регістра L_1. При кожному з них згенеруємо послідовність (x_i), $i = \overline{0, N-1}$, та підрахуємо значення статистики

$$R = (x_0 \oplus z_0) + (x_1 \oplus z_1) + \ldots + (x_{N-1} \oplus z_{N-1}).$$

Позначимо $p := \Pr\{x_i \oplus z_i = 1\}$. Якщо початкове заповнення L_1 вгадано правильно, то, згідно з (3), $p = \frac{1}{4}$, в іншому ж випадку $p = \frac{1}{2}$. Отже, задача зводиться до перевірки гіпотези H_0: $p = p_1 = \frac{1}{4}$ проти альтернативи H_1: $p = p_2 = \frac{1}{2}$ (чому?).

При достатньо великому N розподіл статистики R близький до нормального з параметрами (Np, $\sqrt{Np(1-p)}$) (чому?). Критичну множину вибираємо у вигляді $T_{кр} = \{R > C\}$. При заданій помилці першого роду α (імовірності відкинути H_0, якщо вона вірна) поріг C знаходять за формулою:

$$C = Np_1 + t_{1-\alpha}\sqrt{Np_1(1-p_1)}, \tag{4}$$

де $t_{1-\alpha}$ – квантиль стандартного нормального розподілу.

Відповідний даним значенням C і N квантиль $t_{1-\beta}$ імовірності помилки II-го роду β (імовірності прийняти H_0, якщо має місце H_1) дорівнює:

$$t_{1-\beta} = \frac{Np_2 - C}{\sqrt{Np_2(1-p_2)}}. \tag{5}$$

Таким чином, якщо для даного початкового заповнення L_1 значення статистики $R < C$, вважаємо це заповнення істинним, інакше – відкидаємо його. Необхідну кількість матеріалу N визначають за допомогою нерівності

$$\beta M < 1, \tag{6}$$

де M – кількість варіантів, що випробовуються (в даному випадку $M = 2^{n_1}$). Нерівність (6) означає, що середня кількість обраних за критерієм невірних заповнень L_1 строго менша одиниці (тобто ми фактично унеможливлюємо помилки другого роду). Знайшовши з (6) β, одержуємо систему рівнянь (4) – (5) для визначення величин C та N.

Аналогічно знаходиться заповнення ЛРЗ L_2.

Після цього перебирають всі заповнення регістра L_3 і відбраковують невірні по тактах, на яких $x_i \neq y_i$, а саме: має бути $s_i = 1$, якщо $z_i = x_i$ і $s_i = 0$, якщо $z_i = y_i$.

Зауважимо, що даний метод дозволяє знаходити ключ за $2^{n_1} + 2^{n_2} + 2^{n_3}$ випробувань різних початкових заповнень регістрів. Якщо ж робити повний перебір, тобто перебирати всі можливі початкові заповнення регістрів L_1, L_2, L_3 одночасно і порівнювати одержану послідовність (z_i) із заданою, потрібно розглянути $2^{n_1} \cdot 2^{n_2} \cdot 2^{n_3}$ варіантів.

Порядок виконання роботи

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

1. За даними характеристичними многочленами написати програму роботи ЛРЗ L_1, L_2, L_3 і побудованого на них генератора Джиффі.

2. За допомогою формул (4) – (6) при заданому α визначити кількість знаків вихідної послідовності N^*, необхідну для знаходження вірного початкового заповнення, а також поріг C для регістрів L_1 та L_2.

3. Організувати перебір всіх можливих початкових заповнень L_1 і обчислення відповідних статистик R з використанням заданої послідовності (z_i), $i = \overline{0, N^* - 1}$.

4. Відбракувати випробувані варіанти за критерієм $R > C$ і знайти всі кандидати на істинне початкове заповнення L_1.

5. Аналогічним чином знайти кандидатів на початкове заповнення L_2.

6. Організувати перебір всіх початкових заповнень L_3 та генерацію відповідних послідовностей (s_i).

7. Відбракувати невірні початкові заповнення L_3 за тактами, на яких $x_i \neq y_i$, де (x_i), (y_i) – послідовності, що генеруються регістрами L_1 та L_2 при знайдених початкових заповненнях.

8. Перевірити знайдені початкові заповнення ЛРЗ L_1, L_2, L_3 шляхом співставлення згенерованої послідовності (z_i) із заданою при $i = \overline{0, N-1}$.

Вихідні дані

Характеристичні многочлени:

- для L_1: $p(x) = x^{30} \oplus x^6 \oplus x^4 \oplus x \oplus 1$, що відповідає співвідношенню між членами послідовності $x_{i+30} = x_i \oplus x_{i+1} \oplus x_{i+4} \oplus x_{i+6}$;
- для L_2: $p(x) = x^{31} \oplus x^3 \oplus 1$, відповідна рекурента: $y_{i+31} = y_i \oplus y_{i+3}$;
- для L_3: $p(x) = x^{32} \oplus x^7 \oplus x^5 \oplus x^3 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$s_{i+32} = s_i \oplus s_{i+1} \oplus s_{i+2} \oplus s_{i+3} \oplus s_{i+5} \oplus s_{i+7}.$$

Імовірність помилки першого роду $\alpha = 0{,}01$.

Послідовність (z_i) знаходиться у файлі **`Crypto_CP4_variants_2018.txt`** (обирайте послідовність відповідно до вашого варіанту).

Замість основного варіанту завдання ви можете обрати спрощений варіант завдання. У спрощених варіантах регістри генератору Джиффі визначаються такими характеристичними поліномами:

- для L_1: $p(x) = x^{25} \oplus x^3 \oplus 1$, що відповідає співвідношенню між членами послідовності $x_{i+25} = x_i \oplus x_{i+3}$;
- для L_2: $p(x) = x^{26} \oplus x^6 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$y_{i+26} = y_i \oplus y_{i+1} \oplus y_{i+2} \oplus y_{i+6};$$

- для L_3: $p(x) = x^{27} \oplus x^5 \oplus x^2 \oplus x \oplus 1$, відповідна рекурента:

$$s_{i+27} = s_i \oplus s_{i+1} \oplus s_{i+2} \oplus s_{i+5}.$$

Послідовності (z_i) для спрощених варіантів знаходяться у файлі **`Crypto_CP4_variants_2018_for_dummies.txt`** (обирайте послідовність відповідно до вашого варіанту).

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;
- обчислення та значення параметрів β, C та N^* для перших двох регістрів;
- знайдені початкові заповнення регістрів L_1, L_2 та L_3;
- висновки.

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 запитання

1. Дайте означення потокового шифру, опишіть відмінності між блочними та потоковими шифрами.
2. Дайте означення лінійного регістру зсуву. Чим визначається період регістра? За яких умов період набуває максимального значення?
3. Що таке імпульсна функція?
4. Що таке M-послідовність, які її властивості?
5. Приведіть основні схеми внесення нелінійності у роботу ЛРЗ для криптографічних застосувань. Які вони мають переваги та недоліки?
6. Опишіть схему генератора Джиффі.
7. Опишіть кореляційну атаку на генератор Джиффі. До якого класу атак за рівнем доступної інформації вона відноситься? Які конструктивні недоліки генератора роблять цю атаку успішною?
8. Яка трудомісткість кореляційної атаки на генератор Джиффі в найгіршому випадку?
9. Наведіть алгоритм обчислення параметрів C та N^*. Що станеться, якщо взяти більше (менше) біт гами, ніж N^*? Що станеться, якщо взяти більше (менше) порогове значення C?

Оцінювання комп’ютерного практикуму

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

- реалізація програм – до чотирьох балів (в залежності від правильності та швидкодії); спрощені варіанти оцінюються до трьох балів;
- теоретичний захист роботи – до чотирьох балів;
- несвоєчасне виконання роботи – (-1) бал за кожні два тижні 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.