МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

МЕТОДИЧНІ ВКАЗІВКИ ДО ЛАБОРАТОРНИХ РОБІТ

З ДИСЦИПЛІНИ

«ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ»

(Частина 2)

Одеса — 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

МЕТОДИЧНІ ВКАЗІВКИ
ДО ЛАБОРАТОРНИХ РОБІТ

З ДИСЦИПЛІНИ
«ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ»
(Частина 2)
для студентів інституту інформаційної безпеки, радіоелектроніки та телекомунікацій спеціальності 125 «Кібербезпека»

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та програмного
забезпечення
Протокол № 1 від 27.08.2021

Одеса — 2021

Методичні вказівки до лабораторних робіт з дисципліни «Проблеми кібербезпеки та сучасні підходи до їх вирішення» (Частина 2) для здобувачів інституту інформаційної безпеки, радіоелектроніки та телекомунікацій спеціальності 125 «Кібербезпека» / Укл.: А.В. Соколов. Одеса: «Одеська політехніка», 2021. 19 с.

Укладач: А.В. Соколов

ЗМІСТ

ВСТУП

Дисципліна «Проблеми кібербезпеки та сучасні підходи до їх вирішення» відповідає освітньо-професійній програмі, навчальному та робочому плану підготовки фахівців другого (магістерського) освітньо-професійного рівня вищої освіти за спеціальністю 125 Кібербезпека, і є складовою циклу дисциплін професійної підготовки обов'язкової частини навчального плану.

Предмет дисципліни «Проблеми кібербезпеки та сучасні підходи до їх вирішення» – процеси аналізу кіберзахищеності та синтезу захищених інформаційних систем з використанням сучасних, зокрема авторських, математичних підходів.

Метою дисципліни є забезпечення розвитку фахових компетентностей майбутніх магістрів шляхом оволодіння сучасними підходами до вирішення проблем кібербезпеки.

Завдання вивчення дисципліни:

- Формування у здобувачів загального універсального теоретичного базису для розв'язку різноманітних сучасних проблем в інформаційній та кібербезпеці;
- Набуття практичних навичок застосування теоретичних знань для вирішення конкретних задач, зокрема, в стеганографії, стеганоаналізі, криптографії, виявлення порушень критеріїв захищеності інформації, зокрема її цілісності, що відбувається різноманітними шляхами, в тому числі за допомогою існуючих програмних засобів, програмних середовищ, графічних редакторів, тощо.

Стратегічні цілі дисципліни – націлити майбутніх фахівців на творче застосування, розвиток, удосконалення отриманих знань у подальшій професійній підготовці та їх наступній практичній діяльності.

Мета лабораторних занять полягає у практичному формуванні та розвитку відповідних професійних компетентностей майбутніх фахівців, які слугуватимуть підґрунтям для їхньої практичної роботи, що пов'язана із забезпеченням захисту інформації та організацією інформаційної та кібербезпеки.

Лабораторна робота №1. Моделювання генератора псевдовипадкових ключових послідовностей

Мета роботи — закріпити теоретичні відомості про алгоритм генерації псевдовипадкових ключових послідовностей. Надбати практичні навички виконання операції гамування двійкових повідомлень.

Аудиторне завдання

Нехай задано схему генератора псевдовипадкових ключових послідовностей (рис. 1.1.)

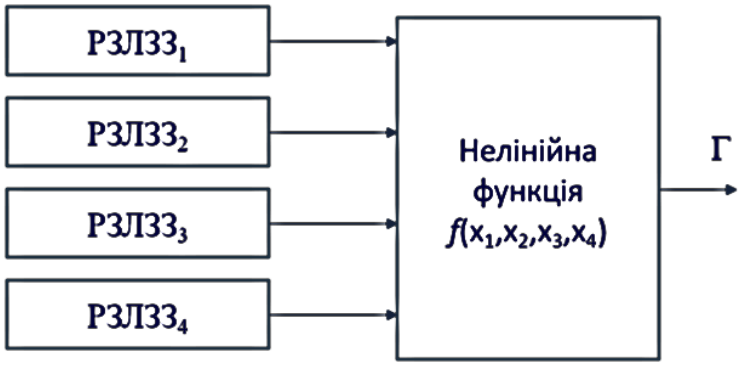

Рис. 1.1. — Схема генератора псевдовипадкових ключових послідовностей

Відомо, що осмислене слово, що належить алфавіту (табл. 1.1) було зашифроване модифікованим шифром Вернама за допомогою гами, згенерованої зазначеним генератором псевдовипадкових ключових послідовностей, в результаті чого була отримана наступна криптограма (табл. 1.3.). При цьому структура РСЛОС визначається генераторними поліномами (табл. 1.2.), а на початку роботи вони мають вихідні стани, що складаються з усіх символів «1». В якості нелінійної булевої функції $f(x_1, x_2, x_3, x_4)$ використовується булева функція, що задана таблицею істинності (табл. 1.2).

Таблиця 1.1.

00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Необхідно:
1. Зашифрувати своє прізвище за допомогою гами згідно варіанту.
2. Розшифрувати своє прізвище за допомогою гами згідно варіанту.
3. Розшифрувати зашифроване повідомлення (табл. 1.3.).

Таблиця 1.2.

№	$g_1(x)$	$g_2(x)$	$g_3(x)$	$g_4(x)$	$f(x_1, x_2, x_3, x_4)$
1	x^3+x^2+1	x^4+x^3+1	x^5+x^3+1	x^6+x^5+1	1 1 0 1 1 0 0 1 1 1 0 1 1 0 1 0
2	x^3+x+1	x^4+x+1	x^5+x^2+1	x^6+x+1	0 0 0 0 0 1 0 0 1 1 0 0 0 0 1 0
3	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^3+x^2+1$	x^6+x^5+1	1 1 1 0 1 0 1 0 0 0 0 1 1 0 1 0
4	x^3+x+1	x^4+x+1	$x^5+x^4+x^3+x+1$	x^6+x+1	1 1 0 0 0 0 0 1 0 0 1 0 1 1 0 1
5	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^2+x+1$	x^6+x^5+1	0 0 1 1 0 0 0 1 1 1 0 1 1 0 0 0
6	x^3+x+1	x^4+x+1	$x^5+x^3+x^2+x+1$	x^6+x+1	0 0 1 1 1 0 0 1 1 0 0 1 0 1 1 1
7	x^3+x^2+1	x^4+x^3+1	x^5+x^3+1	x^6+x^5+1	1 0 1 0 1 0 1 1 1 1 1 0 0 0 1 0
8	x^3+x+1	x^4+x+1	x^5+x^2+1	x^6+x+1	0 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0
9	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^3+x^2+1$	x^6+x^5+1	1 0 1 0 0 0 1 0 0 1 1 1 1 0 1 1
10	x^3+x+1	x^4+x+1	$x^5+x^4+x^3+x+1$	x^6+x+1	0 1 1 0 1 1 1 1 1 1 0 0 1 0 0 0
11	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^2+x+1$	x^6+x^5+1	0 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1
12	x^3+x+1	x^4+x+1	$x^5+x^3+x^2+x+1$	x^6+x+1	1 1 1 0 0 1 0 0 1 0 1 1 1 0 1 1
13	x^3+x^2+1	x^4+x^3+1	x^5+x^3+1	x^6+x^5+1	0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0
14	x^3+x+1	x^4+x+1	x^5+x^2+1	x^6+x+1	1 1 1 0 0 1 0 0 0 0 1 1 0 0 1 0
15	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^3+x^2+1$	x^6+x^5+1	0 1 0 1 1 1 0 0 0 1 0 1 0 0 0 0
16	x^3+x+1	x^4+x+1	$x^5+x^4+x^3+x+1$	x^6+x+1	1 1 0 0 0 1 0 0 0 0 0 0 1 1 0 1
17	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^2+x+1$	x^6+x^5+1	1 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0
18	x^3+x+1	x^4+x+1	$x^5+x^3+x^2+x+1$	x^6+x+1	0 0 1 1 0 1 1 1 1 0 0 1 1 0 0 0
19	x^3+x^2+1	x^4+x^3+1	x^5+x^3+1	x^6+x^5+1	1 1 0 0 0 1 0 0 1 0 0 0 0 0 1 1
20	x^3+x+1	x^4+x+1	x^5+x^2+1	x^6+x+1	0 0 0 1 0 1 1 1 1 1 0 1 0 1 1 0
21	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^3+x^2+1$	x^6+x^5+1	1 0 0 0 1 0 0 0 1 1 1 0 1 0 1 0
22	x^3+x+1	x^4+x+1	$x^5+x^4+x^3+x+1$	x^6+x+1	1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1
23	x^3+x^2+1	x^4+x^3+1	$x^5+x^4+x^2+x+1$	x^6+x^5+1	1 0 0 1 1 0 1 1 0 0 0 0 1 1 1 1
24	x^3+x+1	x^4+x+1	$x^5+x^3+x^2+x+1$	x^6+x^5+1	1 0 0 1 0 1 0 0 1 0 0 0 1 0 0 0

Таблиця 1.3.

№	Шифротекст
1	0 0 0 1 0 0 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 0 0 1 1 1 0 1 1 1 0 1 0 0 1
2	1 1 1 0 0 0 0 0 1 1 0 0 1 0 0 1 0 1 0 1 1 1 0 0 0
3	0 0 1 1 0 0 1 1 0 1 0 1 1 0 0 1 0 0 1 0 0 0 1 0 1 1 1 1 1 1 1 0 0 0 1 1 0 1 0 0 0
4	1 1 1 1 1 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 1 0 1 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 1 1 1 0 1 0 1 0 1 0 0 0 1 0 1 1 0 1
5	0 0 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 1 0 0 1 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 1
6	1 0 1 1 0 0 0 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1 1 0 0 1 1 1 1 0 1 0 0 0 0 0 1 0 1 0
7	0 1 0 0 0 1 0 1 0 1 1 1 0 1 1 0 0 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 0 1 1
8	0 1 0 0 1 1 1 0 0 1 1 1 1 0 0 0 1 1 0 0 0 1 0 1 1 0 0 1 1 1 0 1 0 0 0 0 0 0 1 0 1 0 1 0 1
9	1 0 0 1 0 1 1 1 0 1 1 0 1 0 1 1 0 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0
10	0 1 0 1 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1 1 0 1 0 1 0 1 0 0 1 0 0 1 1 1 0 1
11	1 0 0 0 1 0 0 0 0 0 1 1 1 0 0 1 1 1 1 1 1 1 1 1 0 1 1 1 0 1 1 0 1 0 1 1 0 0 0 0 1 1 0 1 1 0 1 0 0 1 1
12	1 0 0 0 0 0 1 1 1 0 1 1 1 1 1 0 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 1 1 0 0 0 0 0 1 0 0 1 0 0 0 1 0 1
13	0 1 1 0 1 0 1 0 0 1 1 0 1 1 0 1 0 0 0 0 1 1 0 0 0 0 0 1 0 1 0 0 0 0 1
14	0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 1 0 0 0 1 1 0 0 1 0 1 0 0 0 0 0 0 1 1 0 0
15	0 1 1 0 1 0 0 1 1 1 1 1 1 0 1 1 1 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 0 0 0 1 0 1 1 0 0 1

Закінчення табл. 1.3.

16	0 1 1 0 1 0 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 1 0 1 1 1 0 0 1 1 0 1 1 1 0 0 0 1 0 1
17	0 1 1 1 0 1 1 1 0 1 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0
18	1 0 0 1 1 0 1 1 0 0 1 1 1 0 1 1 1 1 0 1 0 0 1 1 1 0 1 1 0 0 1 0 1 1 0 1 0 0 0 0
19	1 0 0 0 1 0 0 0 1 0 0 1 1 1 0 0 1 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 1 1 1 1 1 0 0 1 1 0 0 0 1 0 1 0 0 1 0 1 0 0 1
20	1 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0 1 1 1 1 1 1 0 0 0 0 1 0 1 0 1 1 0 1 0 0 1 0 1
21	0 1 1 0 1 0 1 0 0 1 1 0 1 1 0 0 0 0 1 1 1 1 1 1 1 0 0 1 1 0 0 1 1 1 0 0 0 1 0 0
22	1 0 1 1 0 0 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 1 0 0 0 0 1 1 0 0 1
23	1 0 0 0 0 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 0 0 1 0 0 1 0 0
24	0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 1

Установчий приклад

Нехай задано генераторні поліноми: $g_1(x) = x^3 + x^2 + 1$, $g_2(x) = x^4 + x^3 + 1$, $g_3(x) = x^5 + x^4 + x^2 + x + 1$, $g_4(x) = x^6 + x^5 + 1$,

булева функція $f(x) = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{Bmatrix}$

та шифротекст $\{1\,0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1\}$.

Генеруємо відповідні *m*-послідовності необхідної довжини:

$m_1 = \{1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\}$;

$m_2 = \{1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,0\}$;

$m_3 = \{1\,1\,1\,1\,1\,1\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,1\,1\}$;

$m_4 = \{1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\}$.

Обчислюємо відповідні індекси:

{15 15 15 14 13 10 4 11 3 9 4 11 8 4 1 15 11 6 15 8 10 1 11 15 4},

та знаходимо вихідну послідовність генератора:

$\Gamma = \{0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\}$.

Підсумовуючи отриману послідовність з шифротекстом по модулю 2 отримуємо відкритий текст:

1 0 0 0 1. 1 0 0 1 1. 0 0 1 0 0. 1 1 1 0 0. 1 1 1 1 1,

який відповідає слову «СУДЬЯ».

Контрольні запитання

1. Наведіть визначення та правила побудови регістрів зсуву з лінійним зворотним зв'язком?
2. Які вимоги висуваються до генераторів псевдовипадкових ключових послідовностей?
3. Наведіть алгоритми шифрування та розшифрування за допомогою шифра Вернама.

Рекомендована література

1. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Lap Lambert Academic Publishing, Germany 2015. 100 с.

2. Соколов А. В., Жданов О. Н., Айвазян О. А. Методы синтеза алгебраической нормальной формы функций многозначной логики. Системный анализ и прикладная информатика, 2016. №1. С. 69-76.

3. Дьяконов В. П. MATLAB. Полный самоучитель. М.: ДМК Пресс, 2012. 768 с.

Лабораторна робота №2. Алгоритми уявлення булевих функцій поліномами Жегалкіна

Мета роботи — вивчити основні властивості та криптографічні характеристики булевих функцій, отримати практичні навички уявлення булевих функцій поліномами Жегалкіна.

Аудиторне завдання

1. Знайти обсяги булевих функцій $f(x_1, x_2, \cdots, x_n)$ для значень $n = 1,2,3,4,5,6,7,8$; подати дані у вигляді таблиці.
2. Відповідно до номера варіанта (табл. 2.1.) представити (вручну) функції f_1, f_2 поліномами Жегалкіна (в алгебраїчній нормальній формі) методом невизначених коефіцієнтів і швидким методом множення на квадратну матрицю L. Переконається, що кожен метод дає однакові результати.
3. Перевірити правильність знаходження алгебраїчних нормальних форм булевих функцій f_1, f_2 шляхом обчислення їх таблиць істинності.
4. Визначити такі криптографічні властивості булевих функцій f_i [1]:
   - 4.1. Кількість термів у функції.
   - 4.2. Кількість термів у функції, що містять певну змінну.
   - 4.3. Нелінійний порядок функції (алгебраїчний степінь нелінійності).
   - 4.4. Алгебраїчний степінь кожної змінної.
5. На підставі отриманих криптографічних характеристик заданих булевих функцій провести їхній порівняльний аналіз.

Таблиця 2.1.

N	Функція f_1	Функція f_2	Функції f_3, f_4
1	$f_1 = \{0\,0\,1\,1\,0\,1\,0\,1\}$	$f_2 = \{0\,0\,1\,1\,0\,1\,1\,1\}$	$f_3 = \{1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\}$ $f_4 = \{1\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,1\,0\}$
2	$f_1 = \{0\,0\,1\,1\,1\,0\,1\,1\}$	$f_2 = \{0\,0\,1\,1\,1\,0\,1\,0\}$	$f_3 = \{1\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\}$ $f_4 = \{1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\}$
3	$f_1 = \{0\,0\,1\,1\,1\,1\,0\,0\}$	$f_2 = \{0\,0\,1\,1\,1\,1\,0\,1\}$	$f_3 = \{0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\}$ $f_4 = \{1\,0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,1\}$
4	$f_1 = \{0\,1\,0\,0\,1\,0\,0\,0\}$	$f_2 = \{0\,1\,0\,0\,1\,1\,0\,0\}$	$f_3 = \{0\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0\}$ $f_4 = \{1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\}$
5	$f_1 = \{0\,1\,0\,1\,0\,1\,0\,1\}$	$f_2 = \{0\,1\,0\,1\,0\,1\,0\,0\}$	$f_3 = \{1\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1\}$ $f_4 = \{1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0\}$
6	$f_1 = \{0\,1\,0\,1\,0\,1\,1\,0\}$	$f_2 = \{0\,1\,0\,1\,0\,1\,1\,1\}$	$f_3 = \{0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\}$ $f_4 = \{0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\}$
7	$f_1 = \{0\,1\,0\,1\,1\,0\,0\,1\}$	$f_2 = \{0\,1\,0\,1\,1\,0\,1\,0\}$	$f_3 = \{1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\}$ $f_4 = \{0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,1\}$
8	$f_1 = \{0\,1\,0\,1\,1\,1\,0\,0\}$	$f_2 = \{0\,1\,0\,1\,1\,1\,0\,1\}$	$f_3 = \{1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\}$ $f_4 = \{1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\}$

Закінчення табл. 2.1.

9	$f_1 = \{0\,1\,0\,1\,1\,1\,1\,0\}$	$f_2 = \{0\,1\,0\,1\,1\,1\,1\,1\}$	$f_3 = \{0\,1\,1\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\}$ $f_4 = \{0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,1\}$
10	$f_1 = \{0\,1\,1\,0\,0\,0\,1\,0\}$	$f_2 = \{0\,1\,1\,0\,0\,0\,1\,1\}$	$f_3 = \{1\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\}$ $f_4 = \{1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\}$
11	$f_1 = \{0\,1\,1\,0\,0\,1\,1\,0\}$	$f_2 = \{0\,1\,1\,0\,1\,0\,0\,0\}$	$f_3 = \{1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\}$ $f_4 = \{1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,1\}$
12	$f_1 = \{0\,1\,1\,0\,1\,1\,1\,1\}$	$f_2 = \{0\,1\,1\,1\,0\,0\,0\,0\}$	$f_3 = \{1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\,1\}$ $f_4 = \{1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\}$
13	$f_1 = \{0\,1\,1\,1\,0\,0\,1\,1\}$	$f_2 = \{0\,1\,1\,1\,0\,1\,1\,1\}$	$f_3 = \{1\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\}$ $f_4 = \{0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,1\,1\}$
14	$f_1 = \{0\,1\,1\,1\,1\,1\,0\,0\}$	$f_2 = \{0\,1\,1\,1\,1\,1\,1\,0\}$	$f_3 = \{1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,1\,1\,0\}$ $f_4 = \{0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\}$
15	$f_1 = \{1\,0\,0\,0\,1\,1\,0\,0\}$	$f_2 = \{1\,0\,0\,1\,0\,0\,0\,0\}$	$f_3 = \{1\,1\,0\,1\,1\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\}$ $f_4 = \{1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1\}$

Обчислювальне завдання

Скласти програму на обраній мові програмування, що призначена для уявлення булевих функцій поліномами Жегалкіна для довільного значення n. Знайти коефіцієнти полінома Жегалкіна функцій f_3 та f_4. Окрім векторного уявлення, програма має генерувати рядок, що відповідає поліноміальному уявленню АНФ.

Контрольні запитання

1. Наведіть визначення булевої функції. [2]
2. Якими способами можна визначити булеву функцію? [2]
3. Що таке алгебраїчна нормальна форма подання булевої функції? [1,2]
4. Коротко опишіть процедуру уявлення булевої функції поліномами Жегалкіна методом невизначених коефіцієнтів. [2, с. 51, 3]
5. Опишіть процедуру знаходження коефіцієнтів полінома Жегалкіна швидким методом. [2]
6. Які переваги та недоліки методу невизначених коефіцієнтів та швидкого методу знаходження коефіцієнтів полінома Жегалкіна? [2]
7. Наведіть основні криптографічні характеристики булевих функцій, що прямують з її алгебраїчної нормальної форми. [1]

Література

1. Сергиенко Р. В., Москвиченко И. В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89. Системы обработки информации. Харьков, 2007. №8(66). С. 91-95.
2. Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография. Спб.: НПО «Профессионал». 2004. 478 с.

3. Мазурков М. И., Чечельницкий В. Я., Мельник М. А., Соколов А. В. Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и m–сдвига. Одесса: Труды ОНПУ. 2012. С.179-187.

Лабораторна робота №3. Дослідження відстані нелінійності булевих функцій

Мета роботи — закріпити теоретичні відомості про афінний код, нелінійність булевої функції, отримати практичні навички розрахунку відстані нелінійності булевої функції.

Аудиторне завдання

1. Побудувати лінійний та афінний коди для $n = 3$. Знайти кодову відстань між усіма словами афінного коду. [1]

2. Ручним методом знайти відстань нелінійності для булевих функцій f_1, f_2, заданих згідно з номером варіанта N в табл. 3.1. [2]

3. З отриманих даних провести порівняльний аналіз запропонованих булевих функцій.

Таблиця 3.1.

N	Функція f_1	Функція f_2	Функція f_3, f_4
1	$f_1 = \{1\,0\,0\,0\,1\,0\,1\,1\}$	$f_2 = \{1\,0\,0\,0\,1\,1\,0\,0\}$	$f_3 = \{1\,1\,0\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\}$ $f_4 = \{0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,1\,0\,1\,0\}$
2	$f_1 = \{1\,0\,0\,1\,0\,0\,1\,1\}$	$f_2 = \{1\,0\,0\,1\,0\,1\,1\,0\}$	$f_3 = \{0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\}$ $f_4 = \{1\,1\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\}$
3	$f_1 = \{1\,0\,0\,1\,1\,0\,0\,0\}$	$f_2 = \{1\,0\,0\,1\,1\,0\,0\,1\}$	$f_3 = \{1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,0\}$ $f_4 = \{0\,1\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\}$
4	$f_1 = \{1\,0\,0\,1\,1\,0\,1\,0\}$	$f_2 = \{1\,0\,1\,0\,0\,0\,0\,1\}$	$f_3 = \{1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\}$ $f_4 = \{0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\}$
5	$f_1 = \{1\,0\,1\,0\,0\,1\,0\,1\}$	$f_2 = \{1\,0\,1\,0\,1\,0\,0\,1\}$	$f_3 = \{0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\}$ $f_4 = \{0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\}$
6	$f_1 = \{1\,0\,1\,0\,1\,1\,0\,0\}$	$f_2 = \{1\,0\,1\,1\,0\,0\,0\,0\}$	$f_3 = \{1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,0\,0\}$ $f_4 = \{1\,1\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\}$
7	$f_1 = \{1\,0\,1\,1\,0\,0\,1\,1\}$	$f_2 = \{1\,0\,1\,1\,0\,1\,1\,1\}$	$f_3 = \{0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\}$ $f_4 = \{1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\}$
8	$f_1 = \{1\,0\,1\,1\,0\,1\,1\,0\}$	$f_2 = \{1\,0\,1\,1\,1\,0\,1\,1\}$	$f_3 = \{1\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1\}$ $f_4 = \{0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\}$
9	$f_1 = \{1\,0\,1\,1\,1\,1\,1\,1\}$	$f_2 = \{1\,1\,0\,0\,0\,1\,0\,1\}$	$f_3 = \{1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\}$ $f_4 = \{0\,1\,1\,1\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1\}$
10	$f_1 = \{1\,1\,0\,0\,0\,1\,1\,1\}$	$f_2 = \{1\,1\,0\,0\,1\,0\,0\,1\}$	$f_3 = \{1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\}$ $f_4 = \{1\,0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,1\,0\,0\}$
11	$f_1 = \{1\,1\,0\,0\,1\,0\,1\,0\}$	$f_2 = \{1\,1\,0\,0\,1\,1\,0\,0\}$	$f_3 = \{0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,0\}$ $f_4 = \{0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\}$

Закінчення табл. 3.1.

12	$f_1 = \{1\,1\,0\,0\,1\,1\,1\,1\}$	$f_2 = \{1\,1\,0\,1\,0\,0\,0\,0\}$	$f_3 = \{1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,0\,1\}$ $f_4 = \{0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\}$
13	$f_1 = \{1\,1\,0\,1\,0\,1\,0\,0\}$	$f_2 = \{1\,1\,0\,1\,0\,1\,1\,0\}$	$f_3 = \{1\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,0\,0\,0\,0\,0\}$ $f_4 = \{0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\}$
14	$f_1 = \{1\,1\,0\,1\,1\,0\,1\,0\}$	$f_2 = \{1\,1\,0\,1\,1\,1\,1\,0\}$	$f_3 = \{1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\}$ $f_4 = \{1\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\}$
15	$f_1 = \{1\,1\,1\,0\,0\,0\,1\,1\}$	$f_2 = \{1\,1\,1\,0\,1\,0\,0\,0\}$	$f_3 = \{1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\}$ $f_4 = \{0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\}$

Обчислювальне завдання

Скласти програму на обраній мові програмування, призначену для знаходження відстані нелінійності булевої функції при довільному значенні параметра n. Знайти відстань нелінійності функцій f_3 та f_4.

Контрольні запитання

1. Що таке афінна булева функція? [1,2]
2. Яка потужність афінного коду, лінійного коду? [1,3]
3. Яка кодова відстань афінного коду? [1]
4. Як визначається відстань нелінійності булевої функції? [2]
5. Яке максимальне значення нелінійності булевої функції? [1, 4]
6. Яким видам атак криптоаналізу допомагає протистояти висока відстань нелінійності булевої функції, що застосовується? [1]
7. Яка максимальна відстань нелінійності збалансованої булевої функції? [1]

Рекомендована література

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М: Издательство МЦНМО. 2004. 472 с.
2. Сергиенко Р. В., Москвиченко И. В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89. Системы обработки информации. Харьков, 2007. №8(66). С. 91-95.
3. Мазурков М. И., Чечельницкий В. Я., Мельник М. А., Соколов А. В. Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и m–сдвига. Одесса: Труды ОНПУ. 2012. С.179-187.
4. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89. Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». 2009. С. 5-12.

Лабораторна робота №4. Дослідження критерію розповсюдження помилки та кореляційного імунітету булевих функцій

Мета роботи — закріпити теоретичні відомості про основні показники диференціальної та кореляційної стійкості булевих функцій, отримати практичні навички розрахунку похідних булевої функції, її відповідності критерію розповсюдження помилки та критерію кореляційного імунітету.

Аудиторне завдання

1. Знайти похідні булевої функції f_1 у всіх напрямках u_i одиничної ваги $wt(u_i)=1$.
2. Обчислити коефіцієнти KP розповсюдження помилки щодо всіх напрямків u_i. Визначити, чи відповідає булева функція f_1 строгому лавинному критерію (SAC).
3. Знайти всі підфункції функції f_1. Визначити порядок m кореляційного імунітету KI, якому вона задовольняє.
4. Знайти спектр Уолша-Адамара $W_f(\omega)$, $\omega=\overline{0,7}$ функції f_1. На його підставі визначити порядок кореляційного імунітету KI, якому задовольняє булева функція f_1. Порівняти отриманий результат із результатом, розрахованим під час виконання п. 3.
5. Зробити висновки про кореляційну ефективність функції f_1.
6. Зробити висновки про криптографічні властивості функції f_1.

Таблиця 4.1.

N	Функція f_1	Функція f_2
1	$f_1=\{0\,1\,1\,0\,0\,0\,0\,0\}$	$f_2=\{0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\}$
2	$f_1=\{0\,1\,1\,1\,1\,1\,1\,0\}$	$f_2=\{1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\}$
3	$f_1=\{0\,0\,1\,0\,0\,1\,1\,1\}$	$f_2=\{0\,1\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\}$
4	$f_1=\{1\,0\,0\,1\,1\,0\,0\,1\}$	$f_2=\{0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\}$
5	$f_1=\{1\,0\,1\,0\,1\,1\,0\,0\}$	$f_2=\{0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\}$
6	$f_1=\{0\,1\,0\,0\,0\,0\,1\,0\}$	$f_2=\{0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\}$
7	$f_1=\{1\,0\,1\,1\,1\,1\,0\,1\}$	$f_2=\{1\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\}$
8	$f_1=\{1\,0\,1\,0\,0\,1\,0\,1\}$	$f_2=\{0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\}$
9	$f_1=\{1\,0\,0\,0\,0\,0\,0\,1\}$	$f_2=\{1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\}$
10	$f_1=\{0\,1\,0\,1\,1\,0\,1\,0\}$	$f_2=\{0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\}$
11	$f_1=\{1\,1\,0\,1\,0\,0\,0\,1\}$	$f_2=\{1\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\}$
12	$f_1=\{1\,1\,0\,0\,0\,0\,1\,1\}$	$f_2=\{1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\}$
13	$f_1=\{1\,1\,0\,1\,1\,0\,1\,1\}$	$f_2=\{1\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1\}$
14	$f_1=\{1\,0\,1\,1\,1\,1\,0\,1\}$	$f_2=\{1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\}$
15	$f_1=\{1\,1\,1\,0\,0\,0\,1\,0\}$	$f_2=\{1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\,1\}$

Обчислювальне завдання

1. Скласти програму на обраній мові програмування, призначену для тестування булевої функції на відповідність строгому лавинному критерію. Провести перевірку виконання строгого лавинного критерію функції f_2.
2. Побудувати гістограму розподілення порядку критерія розповсюдження помилки для булевих функцій чотирьох змінних.
3. Скласти програму на обраній мові програмування, призначену для тестування порядку кореляційного імунітету булевої функції (у частотній або часовій області на вибір). Визначити порядок кореляційного імунітету функції f_2.
4. Побудувати гістограму розподілення порядку кореляційного імунітету для булевих функцій чотирьох змінних.

Контрольні запитання

1. Що називається похідною булевої функції за напрямком e_i? [1]
2. Наведіть умову виконання критерію розповсюдження помилки щодо вектора e_i. [1, 2]
3. У якому випадку булева функція відповідає критерію розповсюдження помилки порядку m? [1]
4. Яка фізична сутність строгого лавинного критерію? [1, 3]
5. Як визначити, чи відповідає булева функція строгому лавинному критерію? [3]
6. Що таке спектр Уолша-Адамара булевої функції та яке фізичне трактування його коефіцієнтів? [1]
7. Наведіть визначення кореляційного імунітету порядку m булевої функції. [1, 2]
8. Коротко опишіть процедуру знаходження порядку кореляційного імунітету булевої функції у часовій області. [1]
9. Коротко опишіть процедуру знаходження порядку кореляційного імунітету булевої функції в частотній області. [1, 2]

Рекомендована література

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М: Издательство МЦНМО. 2004. 472 с.

2. Сергиенко Р. В., Москвиченко И. В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89. Системы обработки информации. Харьков, 2007. №8(66). С. 91-95.

4. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89. Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». 2009. С. 5-12.

Лабораторна робота №5. Дослідження правил побудови криптографічних конструкцій підстановки на основі БЛРП

Мета роботи — вивчити і практично опанувати регулярні правила побудови криптографічних конструкцій підстановки (S-блоків підстановки) над розширеними полями Галуа, дослідити криптографічні характеристики одержаних конструкцій підстановки.

Аудиторне завдання

1. Для заданого виду первісного незвідного полінома $f_1(x)$ та первісного елемента Θ_1 (табл. 5.1.), представити (упорядкувати) елементи розширеного поля $GF(2^4)$ у наступних видах (формах) [1]:

1.1. У вигляді степенів первісного елемента Θ^i.

1.2. У вигляді поліномів $r_i(x)$.

1.3. У вигляді двійкових векторів α_i.

1.4. У вигляді десяткових чисел N_i.

1.5. Побудувати багаторівневу лінійну рекурентну послідовність (БЛРП) і сформувати кодуючу (шифруючу) послідовність виду $Q_1 = [0, \text{БЛРП}]$, довжини $N = 16$, з урахуванням якої побудувати структурну схему S-блока підстановки [3, стор. 922].

Таблиця 5.1.

Номер варіанта	Вид полінома $f_1(x)$	Θ_1
1	$x^4 + x + 1$	3
2	$x^4 + x^3 + 1$	4
3	$x^4 + x + 1$	5
4	$x^4 + x^3 + 1$	9
5	$x^4 + x + 1$	11
6	$x^4 + x^3 + 1$	13
7	$x^4 + x + 1$	14
8	$x^4 + x^3 + 1$	3
9	$x^4 + x + 1$	4
10	$x^4 + x^3 + 1$	5
11	$x^4 + x + 1$	9
12	$x^4 + x^3 + 1$	11
13	$x^4 + x + 1$	13
14	$x^4 + x^3 + 1$	3
15	$x^4 + x + 1$	4

2. Користуючись принципом суперпозиції [33, с. 922] визначити вид перетворення: лінійне або нелінійне, яке визначає собою побудований S-блок підстановки.

3. Представити отриманий S-блок підстановки у вигляді компонентних булевих функцій. Застосовуючи розроблене у попередніх лабораторних роботах програмне забезпечення для кожної з отриманих компонентних булевих функцій оцінити її відповідність таким критеріям криптографічної якості: алгебраїчний степінь нелінійності,

відстань нелінійності, відповідність суворому лавинному критерію, відповідність критерію кореляційного імунітету першого порядку.

4. Використовуючи ручний метод дослідити для побудованого S-блока його відповідність таким специфічним для даних криптографічних конструкцій критеріям: критерій рівномірної мінімізації елементів матриці коефіцієнтів кореляції, критерій максимізації періодів повернення, критерій відсутності лінійної надмірності.

Обчислювальне завдання

1. За допомогою обраної мови програмування створити програмне забезпечення, призначене для обчислення матриць коефіцієнтів кореляції S-блоків довільної довжини.

2. За допомогою обраної мови програмування створити програмне забезпечення, здатне на обчислення періодів повернення у вихідний стан для S-блоків довільної довжини.

3. За допомогою обраної мови програмування створити програмне забезпечення, здатне на визначення відповідності S-блока критерію відсутності лінійної надмірності.

Контрольні запитання

1. Наведіть визначення і поясніть аксіоми алгебраїчного поля.[1,4]
2. Що називається періодом елемента поля? [3]
3. Дайте визначення незвідного полінома, первісного полінома. У чому їхня принципова відмінність? [2]
4. Наведіть команди та приклади пошуку в пакеті MATLAB первісних поліномів [6].
5. Що таке автоморфізм та ізоморфізм елементів поля [4]? Поясніть на конкретних прикладах.
6. Як визначається кількість первісних поліномів? Незвідних поліномів? [2]
7. Що таке блок підстановки? Де і з якою метою він застосовується? [5]
8. Які форми представлення S-блоків підстановки Ви знаєте? [4]
9. Поясніть сутність та практичне значення принципу суперпозиції [3].

Рекомендована література

1. Мазурков М. І. Основи теорії передавання інформації. Одеса: Наука і техніка, 2005. 168 с.
2. Мазурков М. И., Конопака Е. А. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа. Радиоэлектроника. 2005. № 11. С. 58 — 65.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Издательский дом "Вильямс", 2003. 1104 с.
4. Свердлик М. Б. Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.
5. Зайко Ю. Н. Криптография глазами физика. Изв. Саратовского ун-та 2009. Т. 9 Вып. 2 С. 34-48.
6. Matlab. Вычисления в конечных полях (полях Галуа). Сайт http://www.matlab.ru /

Лабораторна робота №6. Дослідження відстані нелінійності S-блоків при їх уявленні за допомогою компонентних функцій багатозначної логіки

Мета роботи — закріпити теоретичні відомості про метод уявлення S-блоків за допомогою компонентних функцій багатозначної логіки. Набути практичний досвід розрахунку нелінійності функцій багатозначної логіки.

Аудиторне завдання

1. Уявити заданий згідно до варіанта S-блок всіма можливими способами за допомогою булевих функцій та функцій багатозначної логіки.
2. Використовуючи програмне забезпечення, розроблене у попередніх лабораторних роботах розрахувати значення нелінійності компонентних булевих функцій заданого S-блока підстановки.
3. Розрахувати значення нелінійності компонентних 4-функцій заданого S-блока підстановки.
4. Зробити ґрунтовні висновки щодо нелінійних властивостей заданого S-блока.

Таблиця 6.1.

N	S-блок
1	[0 10 5 1 11 8 2 15 13 9 12 7 3 14 4 6]
2	[10 0 12 13 8 11 6 7 3 15 9 5 4 14 1 2]
3	[2 7 13 0 4 3 9 8 10 15 14 11 12 5 6 1]
4	[10 13 3 11 5 1 9 2 15 4 6 7 8 0 14 12]
5	[5 1 9 3 15 11 10 13 2 6 12 7 8 14 4 0]
6	[12 14 2 6 1 15 13 0 9 11 10 5 4 8 7 3]
7	[2 15 10 0 13 7 9 12 14 1 6 5 11 8 3 4]
8	[8 9 4 0 10 5 6 14 15 3 13 11 12 7 1 2]
9	[8 4 2 0 14 5 12 13 11 15 6 3 1 10 7 9]
10	[13 14 7 4 15 0 6 10 12 11 3 2 5 1 9 8]
11	[14 4 10 2 3 5 0 15 7 9 6 13 1 11 8 12]
12	[14 11 6 5 2 12 7 8 0 9 10 1 3 4 13 15]
13	[15 8 3 13 12 4 1 9 7 6 2 10 11 0 5 14]
14	[3 9 7 4 5 11 10 6 13 8 12 2 0 15 14 1]
15	[3 13 2 14 0 6 5 12 8 9 1 4 11 10 15 7]

Обчислювальне завдання

Використовувана у криптоалгоритмі AES конструкція Ніберг є відображенням у вигляді мультиплікативно зворотних елементів поля Галуа $GF(2^k)$

$$y = x^{-1} \bmod d[f(z), p], \quad y, x \in GF(2^k),$$

яке часто комбінують разом з афінним перетворенням

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{y} + \mathbf{a}, \quad \mathbf{a}, \mathbf{b} \in GF(2^k),$$

де $f(z)$ — незвідний над полем $GF(2)$ поліном;

A — невироджена матриця афінного перетворення;

a — вектор зсуву;

$p = 2$ — характеристика розширеного поля Галуа, $0^{-1} \equiv 0$ — прийнято;

a, b, x, y — елементи розширеного поля Галуа $GF(2^k)$, розглядаються як десяткові числа, або двійкові вектори, або поліноми степеню $k-1$.

Для S-блока конструкції Ніберг (без врахування афінного перетворення), побудованого згідно до незвідного полінома, заданого у табл. 6.2., дослідити нелінійність компонентних функцій багатозначної логіки при всіх його можливих уявленнях (булеві функції, 4-функції, 16-функції).

Таблиця 6.2.

№	Поліном	№	Поліном	№	Поліном
1	285	6	397	11	379
2	301	7	451	12	415
3	351	8	487	13	433
4	357	9	283	14	471
5	369	10	319	15	499

Контрольні запитання

1. Наведіть визначення функції багатозначної логіки?
2. Яким чином S-блок може бути уявлений за допомогою компонентних функцій багатозначної логіки? Наведіть конкретні приклади.
3. Що називається експоненційною формою уявлення функцій багатозначної логіки?
4. Що називається перетворенням Віленкіна-Крестенсона функцій багатозначної логіки?
5. Яким чином можливо вимірити нелінійність функцій багатозначної логіки?

Рекомендована література

1. Sokolov A. V., Zhdanov O. N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. Journal of Telecommunication, Electronic and Computer Engineering, 2016. Vol. 8, No. 9. P. 39-43.

2. Sokolov A. V. Djiofack Temgoua Vanissa Noel. Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019. P. 96—106.

3. Kazakova N. F., Karpinski M., Sokolov A. V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. Procedia Computer Science, 2021. Vol. 192. P. 2731-2741.