МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Криптографические методы защиты информации

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

Изучение булевых функций и их свойств

(тема отчета)

Информационная безопасность (10.03.01)

(код и наименование направления/специальности)

Студент группы ИКБ-03:
Шанин П.С. _____ _____
(Ф.И.О.) *(подпись)*

Д.т.н., проф. каф. ЗСС:
Яковлев В.А. _____ _____
(Ф.И.О.) *(подпись)*

Санкт-Петербург

2023 г

Цель работы: Получение практических навыков по изучению свойств БФ $f(x_1,x_2,x_3)$ и булевых функций, используемых в нелинейном преобразовании алгоритма «Кузнечик» стандарта ГОСТ 34.12-2015.

Используемое программное обеспечение: В работе используется электронный документ «Исследование БФ.xlsx», разработанный в Microsoft Excel – программа для работы с электронными таблицами.

Ход выполнения лабораторной работы:

Часть 1.

Булевой функцией (БФ) называется отображение $\{0,1\}^n \rightarrow \{0,1\}$, т. е. сопоставление вектору из n бит значение 0 или 1. Задать БФ от n переменных можно, указав значение функции на каждом из наборов значений переменных. Булева функция может быть задана таблицей истинности. В лабораторной работе булева функция задана согласно варианту студента в списке группы – 20 вариант.

Таблица 1 – Булева функция

Аргумент			Номер варианта
X3	**X2**	**X1**	**20**
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Вторым этапом выполнения лабораторной работы является нахождение полинома Жегалкина. Любая булева функция может представляться в виде алгебраической нормальной формы – АНФ. Алгебраическую нормальную форму также называют полиномом Жегалкина: $f_n = y_0 \cdot 1 \oplus y_1 \cdot x_1 \oplus y_2 \cdot x_2 \ldots \oplus y_{12} \cdot x_1 \cdot x_2 \ldots \oplus y_{1..n} \cdot x_{1..xn}$.

Заданная БФ:

$$f = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Построили матрицу $A_n = [8*8]$ рекуррентным образом:

$$A_n = \begin{bmatrix} 10000000 \\ 11000000 \\ 10100000 \\ 11110000 \\ 10001000 \\ 11001100 \\ 10101010 \\ 11111111 \end{bmatrix}$$

Для нахождения коэффициентов yi, необходимо перемножить две матрицы A_n и f(x) и от каждого элемент полученной матрицы найти остаток от деления на 2:

$$y = A_n \cdot f = \begin{bmatrix} 10000000 \\ 11000000 \\ 10100000 \\ 11110000 \\ 10001000 \\ 11001100 \\ 10101010 \\ 11111111 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 3 \\ 2 \\ 4 \end{bmatrix} \rightarrow y = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

После перемножения двух матриц получаем столбец коэффициентов y0, y1 … y123. Для более удобного восприятия, запишем столбец в транспонированном виде:

Таблица 2 – Коэффициенты

X1	X2	X3	y	Переменные
0	0	0	0	1
0	0	1	1	x3
0	1	0	0	x2
0	1	1	1	x2x3
1	0	0	1	x1
1	0	1	1	x1x3
1	1	0	0	x1x2
1	1	1	0	x1x2x3

Таким образом, АНФ булевой функции имеет вид:

$$f = x1 \oplus x3 \oplus x1\,x3 \oplus x2\,x3$$

В следующем этапе лабораторной работы необходимо определить вес БФ. Вес БФ - число единиц среди его элементов. Таким образов вес представленной БФ = 4.

Четвёртый этап – найти нелинейность исследуемой БФ. Термин «нелинейность» принят для оценки степени нелинейности, использующей понятия веса и расстояния Хэмминга. Расстоянием Хэмминга это число, равное количеству позиций, в которых различаются соответствующие символы двух функций одинаковой длины т.е., это число позиций, на которых f(x) не равно g(x).

Нелинейность находится по формуле:

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in GF(2)^n} \left| U_a(f^{\wedge}) \right|$$

Для количественной оценки нелинейности в первую очередь необходимо найти спектры Уолша-Адамара (ПУА). $U_a(f)$ это преобразование ПУА от БФ. $U_a(f^{\wedge})$ это ПУА для сопряженной булевой функции, которое представлено в виде:

$$U_a(f) = \sum_{x \in GF(2)^n} f(x)(-1)^{(a,x)}$$

$$U_a(f^{\wedge}) = \sum_{x \in GF(2)^n} (-1)^{(f(x) \oplus (a,x))}$$

где **a** это векторный параметр, принимающие все возможные комбинации 1 и 0.

Первое, что необходимо сделать для нахождения нелинейности БФ это найти скалярное произведение b= (**a**, **x**). Скалярное произведение в координатах ищется по формуле:
$b = a_1x_1; a_2x_2;\ldots;a_nx_n$.

Таблица 3 - Таблица векторов x и a.

	x			a			
x0	0	0	0	0	0	0	a0
x1	0	0	1	0	0	1	a1
x2	0	1	0	0	1	0	a2
x3	0	1	1	0	1	1	a3
x4	1	0	0	1	0	0	a4
x5	1	0	1	1	0	1	a5
x6	1	1	0	1	1	0	a6
x7	1	1	1	1	1	1	a7

Таблица 4 – Скалярное произведение векторов

xi, a0	xi, a1	xi, a2	xi, a3	xi, a4	xi, a5	xi, a6	xi, a7
0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1
0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0
0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	0
0	0	1	1	1	1	0	0
0	1	1	0	1	0	0	1

Таблица 5 – $(f(x) \oplus (a,x)) mod\ 2$

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

0	1	1	0	1	0	0	1

Таблица 6 – (-1) в степени $(f(x) \oplus (a, x)) mod\ 2$

1	1	1	1	1	1	1	1
-1	1	-1	1	-1	1	-1	1
1	1	-1	-1	1	1	-1	-1
1	-1	-1	1	1	-1	-1	1
-1	-1	-1	-1	1	1	1	1
-1	1	-1	1	1	-1	1	-1
-1	-1	1	1	1	1	-1	-1
1	-1	-1	1	-1	1	1	-1

Таблица 7 – Сумма

0	0	-4	4	4	4	0	0

Получаем, что максимальный ПАУ по модулю равен 4: $\max_{a \in GF(2)^n} \left| U_a(f^{¿}) \right| = 4$.

Таким образом нелинейность рассчитывается по формуле:

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in GF(2)^n} \left| U_a(f^{¿}) \right| = 2^{3-1} - \frac{1}{2} \cdot 4 = 4 - 2 = 2$$

Существует граница значений нелинейности:

$$N(f) = 2^{n-1} - 2^{\frac{n}{2}-1} = 2^{3-1} - 2^{\frac{3}{2}-1} = 4 - \sqrt{2} \approx 2,59$$

В следующем этапе лабораторной работы необходимо рассчитать коэффициент корреляции. Коэффициентом корреляции R(i,j) между двумя булевыми функциями называется величина:

R(i,j) = $\frac{1}{2^n} \sum$ (fi*(x ¿· fj*(x)),

где f*(**x**) - сопряженная функция к булевой функции.

Так как функция значение функции f(x) соответствует 20 варианту, следовательно по условию лабораторной работы значение g(x) должно соответствовать 21 варианту.

Таблица 8 – Расчёт коэффициента корреляции

f(x)	g(x)	f*(x)	g*(x)	f*(x) · g*(x)	Сумма ∑	Коэф. корреляции
0	0	1	1	1	4	$R(i,j) = \frac{1}{2^3} \cdot 4 = \frac{1}{2}$
1	1	-1	-1	1		
0	1	1	-1	-1		
0	0	1	1	1		
1	1	-1	-1	1		
1	0	-1	1	-1		
1	1	-1	-1	1		
0	0	1	1	1		

Проверили правильность расчетов, используя электронный документ «Исследование БФ.xlsx» лист №1 (рис.1 – 4).

1. Полином Жегалкина (АНФ)

Для нахождения полинома Жегалкина для булевой функции, сначала необходимо найти произведение матрицы An на исследуемую БФ f(x)

$f_n = y_0 \cdot 1 + y_1 \cdot x_1 + y_2 \cdot x_2 \ldots + y_{12} \cdot x_1 \cdot x_2 \ldots + y_{1..n} \cdot x_{1..n}$

									f(x)	Коэф. [An*f(x)]
An =	1	0	0	0	0	0	0	0	0	0
	1	1	0	0	0	0	0	0	1	1
	1	0	1	0	0	0	0	0	0	0
	1	1	1	1	0	0	0	0	0	1
	1	0	0	0	1	0	0	0	1	1
	1	1	0	0	1	1	0	0	1	1
	1	0	1	0	1	0	1	0	1	0
	1	1	1	1	1	1	1	1	0	0

x1	x2	x3	Слаг. ПЖ	Коэф.	ПЖ
0	0	0	1	0	0
0	0	1	x3	1	x3
0	1	0	x2	0	0
0	1	1	x2x3	1	x2x3
1	0	0	x1	1	x1
1	0	1	x1x3	1	x1x3
1	1	0	x1x2	0	0
1	1	1	x1x2x3	0	0

таблице коэффициентов, записываем А **АНФ = x1+x3+x1x3+x2x3** <--заполнить

Рисунок 1 – Проверка расчёта полинома Жегалкина (АНФ)

2. Вес булевой функции

Для нахождения веса исследуемой БФ, необходимо подсчитать кол-во единиц в последовательности

f(x)
0
1
0
0
1
1
1
0

Вес БФ = 4

Рисунок 2 – Проверка нахождения веса булевой функции

3. Нелинейность булевой функции

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in GF(2)^n} |U_a(f^*)|$$

Вычислим ПУА(преобразование Уолша-Адамара) Ua(f*)для БФ.

	x				a		
x0	0	0	0	a0	0	0	0
x1	0	0	1	a1	0	0	1
x2	0	1	0	a2	0	1	0
x3	0	1	1	a3	0	1	1
x4	1	0	0	a4	1	0	0
x5	1	0	1	a5	1	0	1
x6	1	1	0	a6	1	1	0
x7	1	1	1	a7	1	1	1

Скалярное произведение (xi, ai)								f(x)
xi,a0	xi,a1	xi,a2	xi,a3	xi,a4	xi,a5	xi,a6	xi,a7	
0	0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1	1
0	0	1	1	0	0	1	1	0
0	1	1	0	0	1	1	0	0
0	0	0	0	1	1	1	1	1
0	1	0	1	1	0	1	0	1
0	0	1	1	1	1	0	0	1
0	1	1	0	1	0	0	1	0

f(x) + (xi, ai) mod2							
0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0
0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0
1	1	1	1	0	0	0	0
1	0	1	0	0	1	0	1
1	1	0	0	0	0	1	1
0	1	1	0	1	0	0	1

(-1) в степени f(x) + (xi, ai) mod2							
1	1	1	1	1	1	1	1
-1	1	-1	1	-1	1	-1	1
1	1	-1	-1	1	1	-1	-1
1	-1	-1	1	1	-1	-1	1
-1	-1	-1	-1	1	1	1	1
-1	1	-1	1	1	-1	1	-1
-1	-1	1	1	1	1	-1	-1
1	-1	-1	1	-1	1	1	-1

Σ	0	0	-4	4	4	4	0	0
По модулю	0	0	4	4	4	4	0	0

Макс. ПУА По модулю Ua(f*)	4

Нелинейность =	2

Рисунок 3 – Проверка расчёта нелинейности булевой функции

4. Взаимная корреляция

f(x)	g(x)
0	0
1	1
0	1
0	0
1	1
1	0
1	1
0	0

Споряж. БФ	
f*(x)	g*(x)
1	1
-1	-1
1	-1
1	1
-1	-1
-1	1
-1	-1
1	1

Пр-ие
1
1
-1
1
1
-1
1
1

Общая сумма	4

Корреляция = 0,5

Рисунок 4 – Проверка расчёта коэффициента корреляции

Часть 2.

Исследовать булеву функцию fn(x) (согласно варианту), которая используется в нелинейном преобразовании ГОСТ Р-34.12-2015, на уравновешенность. Булева функция для 20 варианта: f3(x) =11101100101100011001011100010110110101100110101100010110011110011010111101110111100101100100010100001011000111100001110111000011010011101010010100111100111101011000010001110010010000101100110010100011000101101010111111010110000001111110010101000000000101100

Нашли и записали полную АНФ для заданной булевой фикции, используя таблицы произведений функции и матрицы An на странице «АНФ» документа «Исследование БФ.xlsx» (рис.5).

Таблица аргументов								
Десят	x1	x2	x3	x4	x5	x6	x7	x8
0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	0	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	0	0	0	0	0	1	0	1
6	0	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	0	0	0	0	1	0	0	1
10	0	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	0	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	0	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	0	0	0	1	0	0	0	1
18	0	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	0	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	0	0	0	1	0	1	1	1
24	0	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0

коэфф.
1
x1
x2
x3
x4
x5
x6
x7
x8
x1x2
x1x3
x1x4
x1x5
x1x6
x1x7
x1x8
x2x3
x2x4
x2x5
x2x6
x2x7
x2x8
x3x4
x3x5
x3x6
x3x7
x3x8

f0(x)* An	f1(x)* An	f2(x)* An	f3(x)* An
0	0	1	1
0	1	0	0
1	0	0	0
0	1	1	1
1	1	0	0
1	1	0	0
1	1	1	1
0	0	0	1
1	1	1	0
1	0	1	1
0	0	0	0
1	0	0	0
1	1	0	1
0	1	0	1
1	0	0	1
0	0	0	1
1	0	1	0
0	0	1	1
0	0	0	1
1	1	0	1
1	0	0	1
0	0	0	0
0	0	1	1
1	1	0	0
1	0	0	1
0	1	0	0
1	1	1	1

Пример:
АНФ f0(x) = x2+x4+x5+x6+x8+x1x2+x1x4...+x1x3x4x5x6x7x8

Рисунок 5 – Поиск полной АНФ для f3(x)

Полная АНФ:
1+x3+x6+x7+x1x2+x1x5+x1x6+x1x7+x1x8+x2x4+x2x5+x2x6+x2x7+x3x4+x3x6+x3x8+
x4x5+x5x6+x6x7+x7x8+x1x2x3+x1x2x4+x1x2x6+x1x3x4+x1x3x5+x1x3x8+x1x4x5+x1x4x6+
x1x4x8+x2x3x6+x2x4x5+x2x4x7+x2x5x6+x2x5x8+x2x6x7+x2x6x8+x2x7x8+x3x4x5+
x3x4x6+x3x5x6+x3x5x8+x3x6x7+x4x5x8+x4x7x6+x4x6x8+x4x7x8+x5x6x7+x5x7x8+
x1x2x3x6+x1x2x3x7+x1x2x3x8+x1x2x4x5+x1x2x4x6+x1x2x4x7+x1x2x4x8+x1x2x5x7+
x1x3x4x5+x1x3x4x6+x1x3x6x7+x1x3x7x8+x1x4x5x7+x1x4x5x8+x2x3x4x6+x2x3x4x7+
x2x3x4x8+x2x3x5x7+x2x3x5x8+x2x3x6x8+x2x3x7x8+x2x4x5x6+x2x4x5x7+x2x4x6x8+
x2x4x7x8+x2x5x6x7+x2x5x6x8+x2x5x7x8+x3x4x5x7+x3x4x5x8+x3x4x6x8+x3x4x7x8+
x3x5x6x7+x4x5x7x8+x4x6x7x8+x1x2x3x4x7+x1x2x3x5x7+x1x2x3x6x7+x1x2x3x6x8+
x1x2x4x5x6+x1x2x4x5x7+x1x2x4x6x7+x1x2x4x7x8+x1x2x5x6x7+x1x2x5x6x8+x1x3x4x5x7+
x1x3x4x5x8+x1x3x4x6x8+x1x3x6x7x8+x1x4x5x6x7+x1x4x5x6x8+x2x3x4x5x7+x2x3x4x6x8+
x2x3x4x7x8+x2x3x5x7x8+x3x4x5x6x7+x3x5x6x7x8+x4x5x6x7x8+x1x2x3x4x6x8+
x1x2x3x5x6x7+x1x2x3x6x7x8+x1x2x4x5x6x7+x1x2x4x6x7x8+x1x2x5x6x7x8+
x1x3x4x5x6x7+x1x3x4x6x7x8+x1x3x5x6x7x8+x2x3x4x5x6x7+x2x3x4x6x7x8+
x2x4x5x6x7x8+x1x2x3x4x5x6x7+x1x2x3x4x5x6x8+x1x2x3x4x5x7x8+x1x2x3x5x6x7x8

Нашли преобразование Уолша-Адамара и далее нелинейность для функции f3(x) используя лист «ПУА» документа «Исследование БФ.xlsx» (рис.6). Рассчитали границу нелинейности по формуле.

Общая сумма	-16	-16	0	36	-4	20	-4	4	28	4	-4	16	0	0	-32	-8	0	-16	24	4	4
По модулю	16	16	0	36	4	20	4	4	28	4	4	16	0	0	32	8	0	16	24	4	4
Макс. ПУА По модулю Ua(f3*)	**36**																				

Рисунок 6 – Преобразование Уолша-Адамара для f3(x)

Таким образом нелинейность рассчитывается по формуле:

$$N(f)=2^{n-1}-\frac{1}{2}\max_{a\in GF(2)^n}\left|U_a(f^{i})\right|=2^{8-1}-\frac{1}{2}\cdot 36=128-18=110$$

Существует граница значений нелинейности:

$$N(f)=2^{n-1}-2^{\frac{n}{2}-1}=2^{8-1}-2^{\frac{8}{2}-1}=128-8=120$$

Убедились, что коэффициент взаимной корреляции между сопряженными функциями, которые используются в нелинейном преобразовании ГОСТ Р-34.12-2015 равен нулю, используя лист «Вз. Корр.» документа «Исследование БФ.xlsx» (рис.7), рассчитали коэффициент корреляции.

f0(x)	f1(x)	f2(x)	f3(x)
0	0	1	1
0	1	1	1
1	0	1	1
1	0	0	0
1	1	1	1
0	1	1	1
1	0	0	0
0	1	1	0
1	1	0	1
0	0	1	0
0	1	0	1
0	1	0	1
1	1	0	0
1	0	1	0
0	0	1	0
1	0	1	1
1	0	0	1
1	1	1	0
0	0	0	0

f0*(x)	f1*(x)	f2*(x)	f3*(x)
1	1	-1	-1
1	-1	-1	-1
-1	1	-1	-1
-1	1	1	1
-1	-1	-1	-1
1	-1	-1	-1
-1	1	1	1
1	-1	-1	1
-1	-1	1	-1
1	1	-1	1
1	-1	1	-1
1	-1	1	-1
-1	1	-1	1
1	1	-1	1
-1	1	-1	-1
-1	1	1	-1
-1	-1	1	-1
-1	-1	-1	1
1	1	1	1

Пары функций				
0,1	0,2	0,3	1,2	1,3
1	-1	-1	-1	-1
-1	-1	-1	1	1
-1	1	1	-1	-1
-1	-1	-1	1	1
1	1	1	1	1
-1	-1	-1	1	1
-1	-1	-1	1	1
-1	-1	1	1	-1
1	-1	1	-1	1
1	-1	1	-1	1
-1	1	-1	-1	1
-1	1	-1	-1	1
1	-1	-1	-1	-1
-1	1	-1	-1	1
1	-1	1	-1	-1
-1	1	1	-1	-1
-1	-1	1	1	-1
1	1	-1	1	-1
1	1	1	1	1

Общая сумма	**0**
	0
	0
	0
	0

Корреляция = $R(i,i)=\frac{1}{2^n}\sum(fi^*(x)\cdot fj^*(x))$

Рисунок 7 – Взаимная корреляция

Расчёт коэффициента корреляции: $R(i,j)=\frac{1}{2^8}\cdot 0=0$

Коэффициент корреляции отсутствует и это говорит о том, что функции полностью независимы друг от друга.

Вывод: В ходе выполнения лабораторной работы были получены практические навыки по изучению свойств булевых функций $f(x_1,x_2,x_3)$ и булевых функций, используемых в нелинейном преобразовании алгоритма «Кузнечик» стандарта ГОСТ 34.12-2015. Успешно удалось рассчитать полином Жегалкина для булевой функции, определить вес представленной функции. Ещё одним свойством булевой функции является нелинейность. Термин «нелинейность» принят для оценки степени нелинейности, использующей понятия веса и расстояния Хэмминга. С помощью расчёта

взаимной корреляции двух булевых функций смогли установить их независимость друг от друга (в случае если коэффициент равен 0) или зависимость (если коэффициент отличен от 0).