МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»**

Институт Информатики и телекоммуникаций
Направление Информационная безопасность
Профиль Безопасность автоматизированных систем
Кафедра Безопасности информационных технологий

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Вид ВКР: бакалаврская работа

РАСПРОСТРАНЕНИЕ ПОНЯТИЯ КОРРЕЛЯЦИОННОГО ИММУНИТЕТА НА СЛУЧАЙ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

Обучающийся _____ В.С. Курчатова

Руководитель _____ О.Н. Жданов

Ответственный за нормоконтроль _____ Н.И. Чугунова

Допускается к защите

Заведующий кафедрой _____ В.В. Золотарев

«_____» _____ 20__ г.

Красноярск 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»**

Информатики и телекоммуникаций
Безопасности информационных технологий

УТВЕРЖДАЮ
Заведующий кафедрой
_____ В.В. Золотарев
« ____ » _____ 20 ___ г

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

в форме бакалаврской работе
Обучающийся Курчатова Вера Сергеевна
Группа БКБ16-01 Направление 10.03.01
Информационная безопасность
Тема выпускной квалификационной работы Распространение понятия корреляционного иммунитета на случай функций трехзначной логики

Утверждена приказом по университету от _____№_____
Руководитель ВКР – О.Н. Жданов, кандидат физико-математических наук, доцент кафедры БИТ
Исходные данные для ВКР Научные статьи, интернет-ресурсы

Перечень разделов ВКР
1 Базовые определения трехзначной логики
2 Анализ требований и нормативной документации
3 Метод корреляционного иммунитета на случай трехзначныхфункций

Срок сдачи обучающимся первого варианта ВКР – « ___ » _____ 20__ г.
Срок сдачи обучающимся окончательного варианта ВКР – « ___ » _____ 20__ г.

Руководитель ВКР _____ О.Н. Жданов

Задание принял к исполнению _____ В.С. Курчатова

« ___ » _____ 20__ г.

АННОТАЦИЯ

к бакалаврской работе

«Распространение понятия корреляционного иммунитета на случай функций трехзначной логики»

Курчатова Вера Сергеевна

Ключевые слова: трехзначная логика, алгебраическая нормальная форма, алгебраическая иммунность, корреляционный иммунитет, идеальные матрицы.

Целью данной работы является исследование корреляционного иммунитета на случай трехзначных функций для их дальнейшего применения.

Данная цель определила необходимость постановки и решения основных задач:

а) описать трехзначную логику;

б) рассмотреть понятие корреляционного иммунитета;

в) применить корреляционный иммунитет к трехзначной логики.

Предмет исследования – По результатам исследования предложен метод корреляционного иммунитета на случай функций трехзначной логики. Полученные результаты дают возможность лучше узнать о трехзначной логики, что способствует возможности применения трехзначных функций в жизни.

Работа включает: 34 страницы, 15 таблиц, 53 формулы. Использованных источников – 11.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире теория булевых функций занимает важное место. Двухзначная логика используется во многих теоретических областях, так и в прикладных. Цифровые устройства, системы искусственного интеллекта и другие управляющие системы решают сложные задачи, выполняя элементарные двоичные операции и храня данные в виде нулей и единиц.

Поэтому двухзначная логика до сих пор занимает доминирующее положение. Но все меняется, возрастает сложность решаемых задач и, следовательно, технических устройств. Таким образом, необходимо применение многозначной логики.

Также, из-за массового внедрения вычислительной техники растет количество информационных атак. Поэтому криптография подлежит изучению и улучшению.

Чтобы добиться менее трудоемкого решения криптографических задач в криптоанализе появился метод корреляционного иммунитета.

В связи с этим является актуальным рассмотрение корреляционного иммунитета для трехзначных функций.

Таким образом, целью данной работы является исследование корреляционного иммунитета на случай трехзначных функций для их дальнейшего применения.

Для достижения поставленной цели необходимо решить следующие задачи:

а) описать трехзначную логику;

б) рассмотреть понятие корреляционного иммунитета;

в) применить корреляционного иммунитета к функциям трехзначной логики.

1 БАЗОВЫЕ ОПРЕДЕЛЕНИЯ ТРЕХЗНАЧНОЙ ЛОГИКИ

Многозначная логика является одним из опытов расширения границ осознания и формального описания логических связей реального мира. Впервые Я. Лукашевич обратил внимание на многозначность, как способ отображения информации в рассуждениях.

Многозначные логики появились в 20-х годах XX века в работах Поста и Лукасевича. Несколько позднее было предложено ещё несколько многозначных логик, таких как логика Бочвара, логики Гёделя, логика Клини. Изобретение этих логик было мотивировано разными задачами. Так, Лукасевич и Бочвар исходили из философских предпосылок, вводя третье значение в свои логики для формализации неполного или противоречивого знания. Пост и Гёдель руководствовались более техническими соображениями, когда обобщали классическую логику в -значных системах. Клини же просто искал удобный формализм для анализа понятия частично определённой рекурсивной функции.

Однако все эти логики объединяет важная отличительная особенность: в них теоретически заложена концепция, которую называют истинностной функциональностью. Согласно ей, всякое высказывание имеет некоторое значение истинности, и это значение может быть однозначно вычислено некоторой заранее определённой функцией по значениям входящих в это высказывание подвысказываний.

Между многозначной и булевой логикой имеются рад отличий. Например, хорошо известно, что при подстановке одной булевой функции в другую сохраняется существенная зависимость от переменных, а для функций k-значной логики при $k \geq 3$ аналогичное утверждение неверно.

Трехзначная логика (далее как 3 – функция) – это один из видов многозначной логики, её отображение имеет вид: $\{0,1,2\}^k \rightarrow \{0,1,2\}^3$, где 0 – лож, 1 – истина, 2 – неопределенность, а k – количество переменных.

1.1 Функции 3-значной логики. Аналог правила до Моргана

Аналогичным функциям алгебры двузначной логики, можно определить функции 3-значной логики. Значения переменных и самих функций берутся из множества $\mathbb{E}_3 = 0,1,2$. Множество всех таких функций обозначается через $\mathbb{P}_3$.

Как и булевы функции, каждую функцию $f(x_1, \dots, x_n)$ из $\mathbb{P}_3$ можно задать таблицей истинности (таблица 1.1).

Таблица 1.1–Таблица истинности

$x_1 \dots x_n$	$f(x_1, \dots, x_n)$
$0 \dots 0$	$f(x_1, \dots, x_n)$
…	…
$\sigma_1 \dots \sigma_n$	$f(\sigma_1, \dots, \sigma_n)$
…	…
$2 \dots 2$	$f(2, \dots, 2)$

Так же можно обозначить некоторые элементарные функции для 3-значной логики.

Таблица 1.2– Элементарные функции

x	y	$\max(x,y)$	$\min(x,y)$	$x+y(mod\ 3)$	$xy(mod\ 3)$	$x \perp y$	$x \to y$	$x-y$	$V_3(x,y)$
0	0	0	0	0	0	0	2	0	1
0	1	1	0	1	0	0	2	2	2
0	2	2	0	2	0	0	2	1	0
1	0	1	0	1	0	1	1	1	2
1	1	1	1	2	1	0	2	0	2
1	2	2	1	0	2	0	2	2	0
2	0	2	0	2	0	2	0	2	0
2	1	2	1	0	2	1	1	1	1
2	2	2	2	1	1	0	2	0	2

Пусть $p_3(n)$ – число всех функций $f(x_1, \dots, x_n)$ из $\mathbb{P}_3$. Количество различных наборов значений переменных равно 3^n. На каждом из этих наборов функции $f(x_1, \dots, x_n)$может принимать любое из 3^n значений. Следовательно, всего таких функций будет $p_3(n) = 3^{3^n}$. Это число очень быстро растет, например уже в$\mathbb{P}_3$число функций от переменных x_1 и x_2 равно $p_3(n)$= 19683. Все основные понятия, такие, как формула над множеством функций, значение формулы на наборе значений переменных, функция, реализуемая формулой, существенная и несущественная переменные и др., вводится точно так же, как и в двузначной логике, определения почти дословно повторяются. Однако, переменные и функции принимают уже не два значения, а больше. В частности, если известно значение x из $\mathbb{E}_3$, то нельзя определить значение y из $\mathbb{E}_3$ только на основе соотношения $y \neq x$. Это приводит к принципиальным отличиям $\mathbb{P}_3$ от $\mathbb{P}_2$ [8].

Известно, что при подстановке одной булевой функции в другую сохраняется существенная зависимость от переменных. Покажем, что для функций 3-значной логики аналогичное утверждение неверно.

Рассмотрим функцию $\varphi(x_1, x_2)$, заданную таблицей 1.3.

Таблица 1.3– Пример таблицы истинности

x_1	0	1	2
0	0	0	0
1	0	0	0
2	0	0	1

Функция φ принадлежит $\mathbb{P}_3$ и принимает ненулевое значение только на наборе (2,2). Поэтому функция $\varphi\big(x, \varphi(y, z)\big)$ — константа 0, поскольку для любых $\beta,\ \gamma \in \mathbb{E}_3$ выполняется неравенство $\varphi(\beta, \gamma)\ \neq\ 2$.

Рассмотрим следующие «элементарные» функции 3-значной логики [8]:

1. Константы 0,1,2.
2. Тождественная функция x.
3. Отрицания:

– функции $f(x) = \bar{x} = x + 1(mod\ 3)$ – отрицание Поста или циклический сдвиг;

– $f(x) =\sim N(x) = k - 1 - x$ – отрицание Лукасевича;

Эти функции являются обобщениями отрицания в $\mathbb{P}_2$. Функция $N(x)$ является «зеркальным» отражением x. Она обозначается также $\sim x$.

4. Характеристическая функция {2-го рода} $I_i(x)$:
5.

$$I_i(x) = \begin{cases} k - 1, & \textit{если } x = i \\ 0, & \textit{если } x \neq i \end{cases} \qquad (1.1)$$

6. Характеристическая функция {1-го рода} $j_i(x) = 0, 1, 2$:

$$ji(x) = \begin{cases} 1, & \textit{если } x = i \\ 0, & \textit{если } x \neq i \end{cases} \qquad (1.2)$$

Эти функции являются аналогами функции x^σ в $\mathbb{P}_2$.

7. Минимум: Функции $min(x_1, x_2)$ и $x_1 x_2 (mod\ 3)$. Эти функции являются обобщением конъюнкции. Функция $min(x_1, x_2)$ обозначается также $x_1 \wedge x_2$.

8. Максимум: Функция $max(x_1, x_2)$. Она является аналогом дизъюнкции в $\mathbb{P}_2$ и обозначается также $x_1 \vee x_2$.

9. Сложение по модулю 3: $f(x, y) = x_1 + x_2\ (mod\ 3)$.

10. Умножение по модулю 3: $f(x, y) = xy\ (mod\ 3)$.

11. Разность по модулю 3:

$$(x - y) mod\ 3 = \begin{cases} 3 - (y - x), если\ 0 \le x < y \le 2 \\ x - y, \quad если\ 0 \le y \le x \le 2 \end{cases} \tag{1.3}$$

12. Усеченная разность $x \perp y$:

$$x \perp y = \begin{cases} 0, \quad если\ 0 \le x < y \le 2 \\ x - y, \ если\ 0 \le y \le x \le 2 \end{cases} \tag{1.4}$$

13. Импликация $x \supset y$:

$$x \supset y = \begin{cases} 2, \quad если\ 0 \le x < y \le 2 \\ , 2 - x + y, \ если\ 0 \le y \le x \le 2 \end{cases} \tag{1.5}$$

14. Функция Веба:

$$\nu_k(x, y) = (max(x, y) + 1) mod\ 3. \tag{1.6}$$

15. Транспортизация чисел i и j:

$$t_{ij}(x) = \begin{cases} x, если\ x \in \ i, j \\ \ j, если\ x = i \\ \ i, если\ x = j \end{cases} \tag{1.7}$$

где $t_{ij}(x), i, j \in \ 0, 1, 2\ , i \neq j$.

Теорема аналога правила де Моргана:

$$\sim (x_1 \vee x_2) = (\sim x_1) \wedge (\sim x_2) \sim (x_1 \vee x_2) = (\sim x_1) \wedge (\sim x_2) \quad (1.8)$$

Докажем $\sim (x_1 \vee x_2) = (\sim x_1) \wedge (\sim x_2)$.Два случая для $x_1, x_2 \in E_3$

1) $x_1 \geq x_2;\ x_1 \vee x_2 = x_1\ \sim (x_1 \vee x_2) = 2 - x_1 \sim x_1 = 2 - x_1 \sim x_2 = 2 - x_2\ (\sim x_1) \wedge (\sim x_2) = 2 - x_1;$

2) $x_1 < x_2;\ \sim (x_1 \vee x_2) = 2 - x_2\ (\sim x_1) \wedge (\sim x_2) = 2 - x_2.$

Чтобы удостовериться в этих утверждений приведем пример:

$$\sim min(x, y) = max(\sim x, \sim y), \text{ но } \overline{min(x, y)} \neq max(\bar{x}, \bar{y}). \quad (1.9)$$

Упростим выражение, обозначив все элементы через f_i: $f_1 = f_2$и $f_3 \neq f_4$. Теперь можно составить таблицу:

Таблица 1.4– Пример

x	y	$min(x,y)$	f_1	$\sim x$	$\sim y$	f_2	f_3	$\bar{x}$	$\bar{y}$	f_4
0	0	0	2	2	2	2	1	1	1	1
0	1	0	2	2	1	2	1	1	2	2
0	2	0	2	2	0	2	1	1	0	1
1	0	0	2	1	2	2	1	2	1	2
1	1	1	1	1	1	1	2	2	2	2
1	2	1	1	1	0	1	2	2	0	2
2	0	0	2	0	2	2	1	0	1	1
2	1	1	1	0	1	1	2	0	2	2
2	2	2	0	0	0	0	0	0	0	0

Исходя из таблицы 4, можно убедиться, что выражение получается верным. Рассмотрим таблицу 4. Столбцы f_1 и f_2 совпадают, соответственно выполняется равенство $\sim min(x, y) = max(\sim x, \sim y)$, а f_3 и f_4 , разные, соответственно $\overline{min(x, y)} \neq max(\bar{x}, \bar{y})$ верно.

1.2 Поля Галуа

Для работы с информацией при кодировании и декодировании данных все арифметические операции выполняются в полях Галуа. Применяется так называемая полиномиальная арифметика или арифметика полей Галуа [2]. Таким образом, результат любой операции также является элементом данного поля. Конкретное поле Галуа состоит из фиксированного диапазона чисел.

такое поле называется расширенным. $GF(q)$ – обозначение поля Галуа, где $q = p^n$. Для работы с цифровыми данными естественно использовать $p = 2$ в качестве характеристики поля. При $n = 1$ элементом кодовой последовательности будет бит, при $n = 8$ – 8 бит, то есть байт [3]. Однако в данной работе используются с числа 3–логики. В данном случае $p = 3$, а при $n = 1$ получаемтрит – минимальную целую единицу измерения количества информации источников с тремя равновероятными сообщениями.

Таблица 1.5–Операция сложения

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Таблица 1.6–Операция умножения

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

В таблицах 1.5 и 1.6 приведена арифметика полей Галуа для 3-логики.

1.3 Алгебраическая нормальная форма

Алгебраической нормальной формой 3-функции называется полином Ф над Z_q степени $deg(\Phi) < q$ с коэффициентами $a_i \in \{0,1,2\}$, содержащий операции «Сумма по модулю 3» и «Умножение по модулю 3» [1].

Общий вид 3-функции с $k = 2$ и $N = 9$(рисунок 1.2)

$$f = \{f_{00}, f_{01}, f_{02}, f_{10}, f_{11}, f_{12}, f_{20}, f_{21}, f_{22}\} \quad (1.10)$$

Отсюда следует полином АНФ (рисунок 1.3)

$$f(x_1, x_2) = a_{00} + a_{01}x_2 + a_{02}{x_2}^2 + a_{10}x_1 + a_{11}x_1x_2 + a_{12}x_1{x_2}^2 + a_{20}{x_1}^2 + \\ + a_{21}{x_1}^2x_2 + a_{22}{x_1}^2{x_2}^2, \quad (1.11)$$

где, $a_{ij} \in \{0,1,2\}$– искомые коэффициенты.

Чтобы связать искомые коэффициенты с таблицей истинности, необходимо составить следующую систему уравнений:

$$\begin{cases} f_{00} = a_{00}; \\ f_{01} = a_{00} + a_{01} + a_{02}; \\ f_{02} = a_{00} + 2a_{01} + a_{02}; \\ f_{10} = a_{00} + a_{10} + a_{20}; \\ f_{11} = a_{00} + a_{01} + a_{02} + a_{10} + a_{11} + a_{12} + a_{20} + a_{21} + a_{22}; \\ f_{12} = a_{00} + 2a_{01} + a_{02} + a_{10} + 2a_{11} + a_{12} + +a_{20} + 2a_{21} + a_{22}; \\ f_{20} = a_{00} + 2a_{10} + a_{20}; \\ f_{21} = a_{00} + a_{01} + a_{02} + 2a_{10} + 2a_{11} + 2a_{12} + +a_{20} + a_{21} + a_{22}; \\ f_{22} = a_{00} + 2a_{01} + a_{02} + 2a_{10} + a_{11} + 2a_{12} + +a_{20} + 2a_{21} + a_{22}; \end{cases} \quad (1.12)$$

Данную систему уравнений можно представить в виде матрицы:

$$L_9^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \end{bmatrix}. \quad (1.13)$$

Так же для матрицы (1.13) обратная матрица будет выглядеть:

$$L_9 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (1.14)$$

Чтобы найти искомые коэффициенты, можно воспользоваться одной из формул:

$$A = fL_n, f = AL_n. \quad (1.15)$$

Важно отметить, что для 3-функций матрицы прямого и обратного преобразования АНФ не совпадают.

1.4 Аффинные и линейные функции трехзначной логики

Аналогично двоичному случаю, можно ввести понятия линейной и аффинной функции, на основе которых вводится определение нелинейности.

Скажем, что линейной функцией называется трехзначная функция, аналитически задаваемая как [13]

$$\varphi'(x_0, \dots, x_{k-1}) = a_0x_0 + a_1x_1 + \cdots + a_{k-1}x_{k-1}(mod\ q) = \\ = \sum_{i=0}^{k-1} a_ix_i(mod\ q), \quad (1.16)$$

где $a_0, a_1, \dots, a_{k-1} \in \{0,1, \dots, q-1\}$.

Тогда аффинной функцией называется функций аналитического вида [13]

$$\varphi(x_0, \dots, x_{k-1}) = a_0x_0 + a_1x_1 + \cdots + a_{k-1}x_{k-1} + b(mod\ q) = \sum_{i=0}^{k-1} a_ix_i + \\ +b(mod\ q), \quad (1.17)$$

где $a_0, a_1, \dots, a_{k-1}, b \in \{0,1, \dots, q-1\}$.

Можно заметить, что отличием вида аффинных функций от линейных является присутствие члена b. При этом, если $b = 0$, то функция является линейной.

1.5 Вывод

В первой главе были рассмотрены общие понятия трехзначных функций и некоторые отличия двухзначной и трехзначной логики. Также глава включает: определение трехзначных функций, поля Галуа и преобразования в алгебраическую нормальную функцию.

Можно кратко описать шаги нахождения АНФ 3-функций с произвольным количеством переменных:

а) найти матрицу обратного преобразования;

б) найти матрицу прямого преобразования;

в) вычислить искомые коэффициенты.

Далее будут приведен метод корреляционного иммунитета на случай троичных функций.

2 АНАЛИЗ ТРЕБОВАНИЙ И НОРМАТИВНОЙ ДОКУМЕНТАЦИИ

2.1 Основные актуальные угрозы безопасности информации и причин их возникновения

Рассмотрим угрозы, появление которых может быть обнаружено в прикладном программном обеспечении. В банке угроз безопасности информации ФСТЕК [9] для такого типа приложений можно выделить следующие (таблица 2.1).

Таблица 2.1–Угроза внедрения вредоносного кода в дистрибутив программного обеспечения–УБИ.191 [2]

Описание угрозы	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива
Источник угрозы	– внутренний нарушитель с низким потенциалом; – внешний нарушитель с низким потенциалом.
Объект воздействия	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение
Последствия реализации угрозы	– нарушение конфиденциальности; – нарушение целостности; – нарушение доступности.

Согласно банку данных угроз безопасности информации ФСТЭК [9] для криптографических алгоритмов существует следующая угроза – УБИ.003: Угроза анализа криптографических алгоритмов и их реализации. Ее описание представлено в таблице 2.2[2].

Было доказано существование атаки на шифр ГОСТ 28147-89, имеющей сложность в 2^8 (256) раз меньше сложности прямого перебора ключей при условии наличия 2^{64} пар «открытый текст»/»закрытый текст». Данная атака не может быть осуществлена на практике ввиду слишком высокой вычислительной сложности. Более того, знание 2^{64} пар «открытый текст»/»закрытый текст», очевидно, позволяет читать зашифрованные тексты, даже не вычисляя ключа. В большинстве других работ также описываются атаки, применимые только при некоторых предположениях, таких как

определенный вид ключей или таблиц замен, некоторая модификация исходного алгоритма, или же требующие все ещё недостижимых объёмов памяти или вычислений.

Таблица 2.2– Описание угрозы УБИ.003

Описание угрозы	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки
Источники угрозы	Внешний нарушитель со средним потенциалом
Объект воздействия	Метаданные, системное программное обеспечение
Последствия реализации угрозы	– нарушение конфиденциальности; – нарушение целостности.

На данный момент в открытых источниках информация о наличии применимых на практике атак, без использования слабости отдельных ключей или таблиц замен, не обнаружена[9].

2.2 Требования к ключам и таблицам замен

Для программ, выполняющих генерацию ключей и шифрование, уязвимым местами являются слабые ключи, которые переводят открытый текст в себя или побитовую инверсию открытого текста, либо инвертируют часть битов открытого текста, т. е. шифрования как такового не происходит.

Помимо этого, общепринятыми для всех блочных шифров требованиями к ключам шифрования являются следующие:

– ключ должен являться массивом битов, принимающих с равной вероятностью значения 0 и 1 (для 3-логики 0,1,2);

– между битами ключа не должно быть явной или легко обнаруживаемой зависимости, иными словами, в массиве бит должны отсутствовать статистические закономерности. Аналогично для тернарной логики введем требование: между тритами ключа не должно быть легко обнаруживаемой зависимости.

2.3 Вывод

В главе были рассмотрены основные угрозы, связанные с созданием программного обеспечения, предназначенного для шифрования данных. На основе результатов анализа этих угроз было принято решение добавить критерий для ключей – проверка их разреженности. Требования для ключей шифрования выдвинуты на основе известных методов атаки на шифры с использованием современных компьютеров. Выдвинуты требования для таблиц замен. Несмотря на то, что перечисленные выше требования относятся к классическим (бинарным) методам шифрования, в главе 3 будут применяться данные требования, расширенные для тернарной логики. Это обусловлено тем, что в работе нас интересует «похожесть» значений, которые принимает трит, но не важно, какая это разница – 1 или 2[2].

3 МЕТОД КОРРЕЛЯЦИОННОГО ИММУНИТЕТА НА СЛУЧАЙ ТРЕХЗНАЧНЫХ ФУНКЦИЙ

Одним из приемов современного криптоанализа является использование близости (относительно некоторой метрики) криптографических отображений к отображениям, позволяющим свести исходную криптографическую задачу кменее трудоемкой [4]. Яркими примерами этого являются корреляционный и линейный методы криптоанализа. Одна из возможных характеристик, показывающая эффективность этих методов, была названа нелинейностью функции.

У любой функции есть два параметра: число переменных(n) и степень корреляционной иммунности(m). Термин корреляционной иммунности можно определить как: функция, выход которой не коррелирует с совокупностью любыхmвходов.

3.1 Алгебраическая иммунность 3-функций

Приведем пример алгебраической иммунности на случай 3-функций. Для этого понадобиться полином АНФ (1.3), таблица истинности (табл. 1). Так же будет присутствовать определение аннигилятор, что означает $f \cdot g = 0$ или $(f + \{1,2\}) \cdot g = 0$, где $f, g \in V_n$.

Зададим функцию

$$f(x_1, x_2) = x_1 + x_2 \tag{3.1}$$

Найдем для нее аннигилятор.

$$g(x) = a_{00} + a_{10}x_1 + a_{01}x_2 \tag{3.2}$$

$$f(x) \cdot g(x) = (x_1 + x_2)(a_{00} + a_{10}x_1 + a_{01}x_2) = 0 \tag{3.3}$$

Таблица 3.1–Таблица истинности для$f(x) \cdot g(x)$

x_1	x_2	$f(x) \cdot g(x)$
0	0	0
0	1	$a_{00}+a_{01}=0$
1	0	$a_{00}+a_{10}=0$
1	1	$a_{00}+a_{10}+a_{01}=0$
2	0	$a_{00}+2a_{10}=0$
0	2	$a_{00}+2a_{01}=0$

Из таблицы 3.1 следует, что $a_{00}=a_{01}=a_{10}=0$.

Проверим и для функции$(f+1)$

$$(f+1)\cdot g(x)=(x_1+x_2+1)(a_{00}+a_{10}x_1+a_{01}x_2)=0 \quad (3.4)$$

Таблица 3.2–Таблица истинности для $(f+1)\cdot g(x)$

x_1	x_2	$(f+1)\cdot g(x)$
0	0	$a_{00}=0$
0	1	$a_{00}+a_{01}=0$
1	0	$a_{00}+a_{10}=0$

Из таблицы 3.2 следует, что $a_{00}=a_{01}=a_{10}=0$.

И последняя проверка для функции $(f+2)$

$$(f+2)\cdot g(x)=(x_1+x_2+2)(a_{00}+a_{10}x_1+a_{01}x_2)=0 \quad (3.5)$$

Таблица 3.3–Таблица истинности для $(f+2)\cdot g(x)$

x_1	x_2	$(f+2)\cdot g(x)$
0	0	$a_{00}=0$
0	1	$a_{00}+a_{01}=0$
1	0	$a_{00}+a_{10}=0$
1	1	$a_{00}+a_{10}+a_{01}=0$
2	0	$a_{00}+2a_{10}=0$
0	2	$a_{00}+2a_{10}=0$

Из таблицы 3.3 следует, что $a_{00}=a_{01}=a_{10}=0$.

Получается, что степени 1 для трехзначных функций не существует. Тогда попробуем найти g со степенью 2.

$$g(x)=a_{00}+a_{10}x_1+a_{01}x_2+a_{11}x_1x_2+a_{20}{x_1}^2+a_{02}{x_2}^2=0 \quad (3.6)$$

$$f(x) \cdot g(x) = (x_1{+}x_2)(a_{00}{+}a_{10}x_1{+}a_{01}x_2{+}a_{11}x_1x_2 + {+}a_{20}{x_1}^2{+}a_{02}{x_2}^2) = 0 \quad (3.7)$$

Так же составим таблицу истинности (рисунок 3.4).

Таблица 3.4–Таблица истинности для$(f) \cdot g(x)$

x_1	x_2	$(f) \cdot g(x)$
0	0	0
0	1	$a_{00}{+}a_{01} + a_{02} = 0$
1	0	$a_{00} + a_{10} + a_{20} = 0$
1	1	$a_{00} + a_{10} + a_{01} + a_{11} + a_{20} + a_{02} = 0$
2	0	$a_{00} + 2a_{10} + a_{20} = 0$
0	2	$a_{00} + 2a_{01} + a_{02} = 0$
1	2	0
2	1	0
2	2	$a_{00} + 2a_{10} + 2a_{01} + a_{11} + a_{20} + a_{02} = 0$

В соответствии с таблицей 3.4 можно утверждать, что $a_{01} = a_{10} = 0$, так же $a_{02} = a_{20}$ исходя из $f(01), f(02)$ и $f(10), f(20)$. Получим систему уравнений, основываясь на $f(11)$ и $f(22)$: $\begin{cases} a_{00} + a_{11} + a_{20} + a_{02} = 0 \\ a_{11} + a_{20} = 0 \end{cases}$. Тогда Можно сказать, что $a_{02} = -a_{00} = -a_{11}$или $a_{00} = a_{11}$.

Тогда, $n = 2, d = 2$, $f(x) = x_1 + x_2$ и g будет выглядеть следующим образом:

$$g(x) = a_{00}{+}a_{00}x_1x_2{-}a_{00}{x_1}^2{-}a_{00}{x_2}^2 = a_{00}(1{+}x_1x_2{-}{x_1}^2{-}{x_2}^2) \quad (3.8)$$

Подставим в $f(x) \cdot g(x) = 0$:

$$f(x) \cdot g(x) = (x_1{+}x_2)(1 + x_1x_2{-}{x_1}^2{-}{x_2}^2) = 0 \quad (3.9)$$

Таблица 3.5–Таблица истинности для$(f) \cdot g(x)$

x_1	x_2	$(f) \cdot g(x)$
0	0	0
0	1	0
1	0	0
1	1	0
2	0	0
0	2	0
1	2	0
2	1	0
2	2	0

Следовательно, аннигилятором функции $f(x) = x_1{+}x_2$ является функция $g(x) = 1{+}x_1x_2{-}x_1^2{-}x_2^2$.

Для булевых функций алгебраическая иммунность при значении 2 не допускает равенства корреляционного иммунитета нулю. Тогда если 3−функции имеют высокую алгебраическую иммунность, они могут обеспечить хорошую корреляционную иммунность. По возможности построение блоков замен может происходить так: находим 3-функцию с высокой алгебраической иммунностью, используем её значения, при этом переводя числа из троичного представления, например, в двоичное. Тогда, можно сказать, что такой подход может обеспечить наилучшие свойства блоков замен, по сравнению с булевым подходом.

3.2 Корреляционный иммунитет 3-функций

Для начала введем понятие подфункции 3-функции.

Определение 3.1.Подфункцией 3-функции $f(x)$, называется такая функцияf', полученная подстановкой вfзначений из множества $\{0,1,2\}$ вместо некоторых переменных. Если подставим в функцию f константы $\sigma_{i_1}, \dots, \sigma_{i_s}$ вместо переменных $x_{i_1}, \dots, x_{i_s}$ соответственно, то полученная подфункция обозначается как $f_{x_{i_1},\dots,x_{i_s}}^{\sigma_{i_1},\dots,\sigma_{i_s}}$[12].

Для определения независимости входа 3-функции от её входа и для определения корреляционного иммунитета воспользуемся концепциейдисбаланса 3-функции, которая основана на преобразованиях Виленкина-Крестенсона. Остановимся на этом понятии более подробно.

Коэффициенты преобразования Виленкина-Крестенсона можно найти для вектораtпо следующей формуле

$$\Omega = tV' \tag{3.10}$$

где V'−матрица порядка N, равная длине вектора t, а апостроф обозначает транспонирование.

Правило рекуррентного построения матриц Виленкина-КрестенсонаV_{3^L} (3 основание) любого порядка в символической форме представлено в формуле 3.11.

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & (V_{3^{L-1}} + 1)\mathrm{mod}3 & (V_{3^{L-1}} + 2)\mathrm{mod}3 \\ V_{3^{L-1}} & (V_{3^{L-1}} + 2)\mathrm{mod}3 & (V_{3^{L-1}} + 1)\mathrm{mod}3 \end{bmatrix} \quad (3.11)$$

где $V_3 = \begin{bmatrix} z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 \\ z_0 & z_2 & z_1 \end{bmatrix}$, а суммирование z_i производится по модулю 3.

После построения матрицы Виленкина-Крестенсона в символической форме осуществляется переход к экспоненциальной форме в соответствии со следующими соотношениями $z_0 = e^{j0}$, $z_1 = e^{j2\pi/3}$, $z_2 = e^{j4\pi/3}$.

Дисбаланс 3-функции представляет собой абсолютное значение первого коэффициента преобразования Виленкина-Крестенсона, то есть сумму поэлементного произведения 3-функции на последовательность.

Определение 3.2.Пусть $|i|-$ количество элементов i. Учитывая формулу нахождения модуля комплексного числа, значение дисбаланса Δ последовательности над алфавитом $\{0,1,2\} \leftrightarrow \{z_0, z_1, z_2\}$ определим как [11]:

$$\Delta_f = \sqrt{(1 \cdot |0| - 0.5(|1| + |2|))^2 + \left(\frac{\sqrt{3}}{2}|1| - \frac{\sqrt{3}}{2}|2|\right)^2}. \quad (3.12)$$

Определение 3.3.Говорят, что выход 3-функции $f(x)$ является независимым от группы своих входных переменных $\{x_i\}, i = 1, \dots, m$, если при подстановке вместо этих переменных любых констант $\sigma_{i_1}, \dots, \sigma_{i_s} \in \{0,1,2\}$, дисбаланс полученных таким образом подфункций составляет $\Delta_{f'} = \frac{\Delta_f}{3^m}$ [11].

Определение 3.4.Говорят, что 3-функция $f(x)$ является корреляционно иммунной порядка $m \leq k$, если её выход является независимым относительно любой группы их m своих входных переменных, то есть дисбаланс всех её подфункций $k - m$переменных составляет $\Delta_{f'} = \frac{\Delta_f}{3^m}$ [12].

Пример.Зададим 3-функцию порядка $m = 2$

$$f = \left\{\frac{x_1x_2x_3{:}000\ 001\ 002\ 010\ 011\ 012\ 020\ 021\ 022}{f(x_1x_2x_3){:}0\ 2\ 1\ 1\ 0\ 2\ 2\ 1\ 0}\right\} \tag{3.13}$$

$$\Delta(0\ 2\ 1\ 1\ 0\ 2\ 2\ 1\ 0) = \sqrt{(1\cdot 3 - 0.5(3+3))^2 + \left(\frac{\sqrt{3}}{2}3 - \frac{\sqrt{3}}{2}3\right)^2} = 0 \tag{3.14}$$

Получается, данная функция является сбалансированной. По определение 3.4 для независимости данной функции от какой-либо из своих переменных, необходимо, чтобы её подфункции, полученные путем подстановки в данные переменные любых констант, были сбалансированы. Так как $m = 2$, то подфункций будет с $k - m = 3 - 2 = 1$ переменной.

$$\begin{array}{lll} f(0,0,x_3) = \left\{\frac{000\ 001\ 002}{0\ 2\ 1}\right\} & f(0,x_2,0) = \left\{\frac{000\ 010\ 020}{0\ 1\ 2}\right\} & f(x_1,0,0) = \left\{\frac{000\ 100\ 200}{0\ 1\ 2}\right\} \\ f(0,1,x_3) = \left\{\frac{010\ 011\ 012}{1\ 0\ 2}\right\} & f(0,x_2,1) = \left\{\frac{001\ 011\ 021}{2\ 0\ 1}\right\} & f(x_1,0,1) = \left\{\frac{001\ 101\ 201}{2\ 0\ 1}\right\} \\ f(0,2,x_3) = \left\{\frac{020\ 021\ 022}{2\ 1\ 0}\right\} & f(0,x_2,2) = \left\{\frac{002\ 012\ 022}{1\ 2\ 0}\right\} & f(x_1,0,2) = \left\{\frac{002\ 102\ 202}{1\ 2\ 0}\right\} \end{array} \tag{3.15}$$

Проанализировав множество (3.7), можно сказать, что все подфункции одной переменной 3-функции (3.5) имею нулевой дисбаланс ($\Delta_{f'} = 0$). И так как $\Delta_f = 0$, то данная 3-функция является корреляционно-иммунной 2 порядка.

3.3 Корреляционный иммунитет 3-функций от двух переменных

Для анализа корреляционного иммунитеты порядка $m = 1$ для 3-функций двух переменных рассмотрим подфункции $m = 1$ переменной, где таблица истинности составляет $n = 3$.

Рассмотрим полное множество 3-функций и мощность $J = 3^n = 3^3 = 27$ и определим возможные значения дисбаланса 3-функций в представленном множестве [11].

Δ	J_Δ
0	6
$\sqrt{3}$	18
3	3

(3.16)

Получается, что корреляционно иммунными 1 порядка могут быть только 3-функции$N = 9$. В соответствии с определением 3.3 для одной переменной получаем, что для двух переменных необходимо, чтобы дисбаланс был равным $\Delta_f = 3^m\Delta_f, = 3^1\Delta_f, \in \{0,3,9\}$.

Получились следующие результаты, приведенные в таблице 3.1.

Таблица 3.1–Кардинальность 3-функциональных наборов с заданными корреляционными свойствами [11]

Корреляционный иммунитет	Функции, независимые от переменной x_1	Функции, независимые от переменной x_2	3-функции с корреляционным иммунитетом порядка $m=1$
$\Delta = 0,\ J = 1680$			
Количество 3-функций	216	216	12
$\Delta = 3,\ J = 4158$			
Количество 3-функций	972	972	216
$\Delta = 9,\ J = 3$			
Количество 3-функций	3	3	3

Обозначим некоторые правила для метода синтеза таких 3-функций.

Правило 1. Синтез сбалансированных $(\Delta = 0)$ 3-функцийдлины $N = 9$, которые независимы от значения x_1.

Рассмотрим тривиальную монотонно возрастающую последовательность натуральных чисел $\alpha = \{012\}$. Сформируем на её основе множество последовательностей длины $N = 9$ мощности $J_1 = 6^2 = 36$ по следующему правилу

$$A = \{P_i(\alpha)P_j(\alpha)P_l(\alpha)\}, i, j, l = 1, \dots, 6, [12] \quad (3.17)$$

где P – операция применения одной из шести перестановок элементов последовательности

$$P = \begin{Bmatrix} \{123\} & \{231\} \\ \{132\} & \{312\} \\ \{213\} & \{321\} \end{Bmatrix}. \quad (3.18)$$

Если выбрать перестановки $P_i = P_j = P_l = \{123\}$, то получим первую последовательность, выход которой не зависит от входа x_1

$$T_l = \{0\ 1\ 2\ 0\ 1\ 2\ 0\ 1\ 2\}. \quad (3.19)$$

Правило 2. Синтез сбалансированных $(\Delta = 0)$ 3-функций длины $N = 9$, которые независимы от входаx_2 [11].

Полное множество 3-функций, выход которых не зависит от входа x_2, может быть построено на основе полного множества 3-функций, выход которых не зависит от входа x_1 путем простой замены переменных.

Рассмотрим замену переменных $x_1 \leftrightarrow x_2$ на примере последовательности (таблица 3.2).

Таблица 3.2 – Последовательность 3-функций

	0	1	2	3	4	5	6	7	8
x_1x_2	00	01	02	10	11	12	20	21	22
$f(x_1x_2)$	0	1	2	0	1	2	0	1	2
↓									
	0	3	6	1	4	7	2	5	8
x_2x_1	00	10	20	01	11	21	01	12	22
$f(x_1x_2)$	0	0	0	1	1	1	2	2	2

Перестановка $P = \{0,3,6,1,4,7,2,5,8\}$ подтверждает правило перехода от 3-функций, выход которых не зависит от входа x_1 ко множество 3-функций, выход которых не зависит от входа x_2.

Правило 3. Синтез сбалансированных $(\Delta = 0)$ корреляционно-иммунных 1 порядка для 3-функций длины$N = 9$ [11].

Это правило можно описать последовательностью с помощью следующих шагов.

Шаг 1. Рассмотрим монотонно возрастающую последовательность натуральных чисел $\alpha = \{012\}$,на основе которой сформируем 6 последовательностей длины $N = 9$ с помощью следующих правил

$$A_1 = \{\alpha \leftarrow (i+0), \alpha \leftarrow (i+1), \alpha \leftarrow (i+2)\}, i \in \{0,1,2\};$$
$$A_2 = \{\alpha \leftarrow (i+0), \alpha \leftarrow (i+2), \alpha \leftarrow (i+1)\}, i \in \{0,1,2\};^{[12]} \quad (3.20)$$

где символ $\alpha \leftarrow (i+0)$ обозначает оператор циклического сдвига вектора α вправо на величину $(i+0)$.

Шаг 2. К последовательностям, полученным на 1 шаге, применяем операцию замены символов $\{1 \leftrightarrow 2{,}2 \leftrightarrow 1\}$, таким образом, получая из каждой корреляционно-иммунный 3-функции 2 корреляционно-иммунные 3-функции.

Правило 4. Синтез 3-функций длины $N = 9$ дисбаланса $\Delta = 3$, выход которых независим от входа x_1 ивхода x_2[12].

Введем определение опорной 3-функции. Функция

$$s(g, X) = sup_{x \in X}\langle x, g\rangle, g \in \mathbb{R}^n, \tag{3.21}$$

где множество $X \subset \mathbb{R}^n$ непустое и выпуклое, называется опорной функций множества X.

Можно отметить, что полное множество 3-функций длины $N = 9$, которые независимы от входа x_1 и имеет дисбаланс $\Delta = 3$ может быть синтезировано на основе 36 опорных 3-функций[11]

{001001022}	{002011011}	{022001001}	{112022112}
{001001112}	{002122002}	{022001022}	{112112001}
{001022001}	{002122122}	{022022001}	{112112022}
{001022022}	{011002002}	{022022112}	{122002002}
{001112001}	{011002011}	{022112022}	{122002122}
{001112112}	{011011002}	{022112112}	{122011011}
{002002011}	{011011122}	{112001001}	{122011122}
{002002122}	{011122011}	{112001112}	{122122002}
{002011002}	{011122122}	{112022022}	{122122011}

(3.22)

Каждая из опорных последовательностей (матрица3.22) может быть представлена в виде конкатенации (операция подобная умножению, то есть результат конкатенации объектов A и B является объект $C = A \cdot B$, где поочередно добавляются элементы объекта B, начиная с первого, в конец объекта А) трех подпоследовательностей следующим образом[11]:

$$\begin{aligned} A &= \{a_1a_2a_3a_4a_5a_6a_7a_8a_9\} = \{\alpha\ \beta\ \gamma\}, \\ \alpha &= \{a_1a_2a_3\}, \beta = \{a_4a_5a_6\}, \gamma = \{a_7a_8a_9\}. \end{aligned} \tag{3.23}$$

На основе каждой опорной последовательностей (формула 3.23) могут быть построены 27 новых последовательностей путем всех возможных

циклических сдвигов подпоследовательностей α, β, γ ,путем применения следующей конструкции[11]:

$$A = \{\alpha \leftarrow i, \beta \leftarrow j, \gamma \leftarrow l\}, i, j, l = 0,1,2. \quad (3.24)$$

Синтез 3-функций, которые независимы от входа x_2 и имеют дисбаланс$\Delta = 3$, возможен на основе синтезированного полного множества 3-функций, которые независимы от входа x_1 и имеют дисбаланс $\Delta = 3$ путем замены переменных x_1и x_2согласно 3 правилу.

Правило 5.Синтез корреляционно-иммунных порядка $m = 1$ 3-функций длины$N = 9$, которые имеют дисбаланс$\Delta = 3$ [11].

Непосредственными вычислениями установлено, что полное множество корреляционно-иммунных порядка $m = 1$ 3-функций длины $N = 9$, которые имеют дисбаланс $\Delta = 3$ может быть синтезировано на основе 72 опорных 3-функций:

{001001112}	{002110110}	{011002101}	{020110011}
{001001220}	{002122020}	{011011122}	{020122002}
{001010211}	{002200212}	{011011200}	{020200221}
{001022202}	{002212200}	{011020110}	{020212020}
{001100121}	{002221002}	{011101002}	{020212212}
{001112001}	{002221221}	{011110020}	{020221200}
{001112112}	{010001211}	{011122011}	{022001202}
{001121100}	{010010121}	{011122122}	{022010220}
{001202022}	{010010202}	{011200011}	{022022100}
{001211010}	{010022220}	{011200200}	{022022211}
{001220001}	{010100112}	{011212221}	{022100022}
{001220220}	{010112100}	{011221212}	{022100100}
{002002110}	{010121010}	{020002122}	{022112121}
{002002221}	{010121121}	{020011110}	{022121112}
{002011101}	{010202010}	{020020101}	{022202001}
{002020122}	{010202202}	{020020212}	{022211022}
{002101011}	{010211001}	{020101020}	{022211211}
{002110002}	{010220022}	{020101101}	{022220010}

(3.25)

На основе каждой из 72 последовательностей (матрица3.25) могут быть построены 3 последовательности в соответствии со следующим правилом[11]:

$$A = \{a_i\} = \{(A + i) mod\ 3\}, i = 0,1,2 \quad (3.26)$$

Предложение 1.Множество идентичных 3-функций

$$\{000000000\}\ \{111111111\},\ \{222222222\} \tag{3.27}$$

составляют полное множество корреляционно-иммунных 1 порядка 3-функций длины $N = 9$ и они же совпадают с множеством 3-функций длины $N = 9$, которые независимы от входа x_1 или x_2 и имеют дисбаланс Δ=9.

3.4 S-блоки с идеальными матрицами коэффициентов корреляции

С точки зрения S-блоков наибольший интерес представляют собой 3-функции. Проведенные исследования показали, что конструирование полного множества S-блоков возможно на основе 44-х 3-функций, среди которых 12 функций, выход которых не зависит от входа x_1 и еще 12 независимых от входа x_2 (матрицы 3.28, 3.29 соответственно)

$$\begin{matrix}\{012120120\}\ \{021021210\}\ \{102102210\}\ \{120012120\}\ \{201012201\}\ \{210021021\}\\ \{012201201\}\ \{021210021\}\ \{102210102\}\ \{120120012\}\ \{201201012\}\ \{210102102\}\end{matrix} \tag{3.28}$$

$$\begin{matrix}\{002221110\}\ \{020212101\}\ \{101212020\}\ \{112001220\}\ \{200122011\}\ \{211100022\}\\ \{011122200\}\ \{022100211\}\ \{110221002\}\ \{121010202\}\ \{202010121\}\ \{220001112\}\end{matrix} \tag{3.29}$$

Кроме этого состав полного множества S-блоков длины $N = 9$, обладающих идеальными корреляционными матрицами входит 12 корреляционно-иммунных 3-функций порядка$m = 1$ (матрица 3.30), а также 8 функций общего вида (матрица 3.31)

$$\begin{matrix}\{012120201\}\ \{021102210\}\ \{102021210\}\ \{120012201\}\ \{201012120\}\ \{210021102\}\\ \{012201120\}\ \{021210102\}\ \{102210021\}\ \{120201012\}\ \{201120012\}\ \{210102021\}\end{matrix} \tag{3.30}$$

$$\begin{matrix}\{011221020\}\ \{020221011\}\ \{112100202\}\ \{202100112\}\\ \{020122110\}\ \{110122020\}\ \{202001211\}\ \{211001202\}\end{matrix} \tag{3.31}$$

На основе исследовании полного множества из $J = 264$S-блоков длины $N = 9$, обладающих идеальными матрицами коэффициентов корреляции, позволили сформулировать утверждение.

Утверждение 1. Условия идеальной матрицы коэффициентов корреляции предполагают, чтобы хотя бы одна из его компонентных 3-функций была независима от входной переменной x_1 и хотя бы одна из его компонентных 3-функций была независима от входной переменной x_2и по крайней мере один из компонентов S-блока должен быть корреляционно иммунным порядка$m = 1$ [11].

Полное множество $J = 264$S-блоков длины $N = 9$ можно представить в виде объединения пяти классов[11]:

1. S-блоки, у которых выход первой и второй компонентных 3-функций являются независимы от входа x_1 (мощность данного класса S-блоков составляет$J = 48$).

{057624813} {156372480} {318426750} {462570138} {615237804} {750318426}
{057813624} {156480372} {318750426} {462138570} {615804237} {750426318}
{075264831} {237615804} {372480156} {480372156} {624057813} {813624057}
{075831264} {237804615} {372156480} {480156372} {624813057} {813057624}
{084273651} {264075831} {426318750} {516408732} {651273084} {831264075} (3.32)
{084651273} {264831075} {426750318} {516732408} {651084273} {831075264}
{138462570} {273084651} {408516732} {570462138} {732408516} {804237615}
{138570462} {273651084} {408732516} {570138462} {732516408} {804615237}

2. S-блоки, у которых выход первой и второй компонентных3-функций являются независимыми от входа x_2 (мощность данного класса S-блоков составляет$J_2 = 48$).

{026875431} {145367820} {314758260} {451673208} {620578134} {745301286}
{028763541} {154376802} {341785206} {457013862} {628130574} {754310268}
{062857413} {206785341} {347125860} {473251608} {602587143} {826031475}
{068521743} {208673451} {374152806} {475031826} {608251473} {820367145}
{082736514} {260758314} {413857062} {514736082} {682103547} {862013457} (3.33)
{086512734} {268310754} {415637280} {541763028} {680215437} {860125347}
{134578620} {280637415} {431875026} {547103682} {734512086} {802376154}
{143587602} {286301745} {437215680} {574130628} {743521068} {806152374}

3. S-блоки, у которых первая компонентная 3-функции корреляционно-иммунная порядка $m = 1$, а вторая компонентная 3-функция является функцией общего вида (выход которой является корреляционно зависимым от каждого из входов), (мощность данного класса S-блоков составляет $J_3 = 48$).

{047581623} {173428650} {317284650} {472136805} {614257380} {742163508}
{056482713} {175406832} {326185740} {470158623} {623158470} {740185326}
{056824371} {238460715} {326851074} {517064832} {623581047} {814037562}
{074851326} {238604571} {371824056} {508163742} {641527083} {832406175}
{083527641} {247361805} {380257614} {508631274} {650428173} {832064517} (3.34)
{083752416} {265307841} {380725146} {562037814} {650284317} {841307265}
{146725380} {265730418} {416752083} {562703148} {713482056} {805361247}
{148703562} {274631508} {418730265} {571604238} {715460238} {805136472}

4. S-блоки, у которых первая компонентная 3-функция является функцией общего вида (выход которой является корреляционно зависимым от каждого из входов), а вторая компонентная 3-функция является корреляционно-иммунной порядка $m = 1$ (мощность данного класса S-блоков составляет$J_4 = 48$).

{045783261} {162387540} {270468351} {450378261} {627510438} {708321546}
{054873162} {162873054} {270684135} {456312807} {627105843} {708213654}
{072486531} {180567342} {342567180} {531486072} {645123807} {816402357}
{072864153} {180675234} {348501726} {537420618} {654213708} {816024735}
{081576432} {234675180} {351468270} {540387162} {726501348} {834015726} (3.35)
{081765243} {243765081} {357402816} {546321708} {726015834} {843105627}
{135684270} {261378450} {432576081} {618420537} {735024816} {807312456}
{153864072} {261783045} {438510627} {618204753} {753204618} {807123645}

S-блоки, укоторых обе компонентные 3-функции являются корреляционно-иммунными порядка $m = 1$(мощность данного класса S-блоков составляет $J_4 = 72$).

{048561723} {165327840} {318750264} {462057813} {615480237} {750318264}
{048723561} {165840327} {318264750} {462813057} {615237480} {750264318}
{057462813} {183507642} {327165840} {480237615} {624138570} {705381246}
{057813462} {183642507} {327840165} {480615237} {624570138} {705246381}
{075426831} {237480615} {372156804} {516084732} {642183507} {813462057}
{075831426} {237615480} {372804156} {516732084} {642507183} {813057462}
{084516732} {246381705} {381705246} {507183642} {651408273} {831426075} (3.36)
{084732516} {246705381} {381246705} {507642183} {651273408} {831075426}
{138570624} {264318750} {426075831} {561048723} {723561048} {840327165}
{138624570} {264750318} {426831075} {561723048} {723048561} {840165327}
{156372804} {273408651} {408651273} {570624138} {732516084} {804372156}
{156804372} {273651408} {408273651} {570138624} {732084516} {804156372}

Очевидно, чтоS-блоки являются, наиболее, устойчивыми к корреляции криптоанализа, так как их выход независим в то же время от каждой из входных переменных. Эти S-блоки могут быть рекомендованы для

практического использования в приложениях, где требуется максимальная независимость выхода криптографических структур от их ввода.

3.5 Вывод

В третьей главе были рассмотрены: понятие алгебраическойиммунности, где приведен пример функции анигилятора, определение корреляционного иммунитета и его реализации для случая с одной переменно и двух переменных.

ЗАКЛЮЧЕНИЕ

Исследование 3-функций является актуальной темой, в которой многие вопросы нуждаются в более глубокой доработке, например: корректирующие коды, поиск слабых таблиц подстановок, адаптация программных средств, ориентированных на работу с многозначной логикой.

В работе представлены примеры алгебраической иммунности и корреляционной иммунноститрехзначных функций. А так же в первой главе введены некоторые основные понятия, с помощью которых были реализованы выше сказанные примеры.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Жданов, О.Н. Метод синтеза алгебраической нормальной формы функций многозначной логики / А.В. Соколов, О.Н. Жданов, О.А. Айвазян– Одесса, СибГАУ им. М.Ф. Решетнева – С.70-73. – Текст: непосредственный.

2. Неб, А.В. Исследование алгебраической степени нелинейности подстановочных конструкций, основанных на нормальной форме функций многозначной логики / А.В. Неб, О.Н. Жданов – Красноярск, СибГАУ им. М.Ф. Решетнева, 2018 – С. 8-9. – Текст: непосредственный.

3. Подсчет расстояния Хэмминга на большом наборе данных – Текст: электронный // URL: https://habr.com/post/211264/(дата обращения 13.02.2020).

4. Алексеёв, Е.К. Теоретические основы прикладной дискретной математики/Е.К. Алексеёв – Москва: Московский государственный университет им. М. В. Ломоносова, 2011 – С. 5-10. – Текст: непосредственный.

5. Селезнева, С.Н. О сложности обобщенных полиномов k-значных функций/С.Н. Селезнева, А.Б. Дайняк – Москва, ВЕСТН. МОСК. УН-ТА. СЕР. 15. ВЫЧИСЛ. МАТЕМ. И КИБЕРН., 2008 – С. 34-35. – Текст: непосредственный.

6. Халявин,А.В. Оценка нелинейности корреляционно-иммунных булевых функций / А. В. Халявин. – Москва, Московский государственный университет им. М. В. Ломоносова, 2011 – С. 35-36.–Текст: непосредственный.

7. Алексеев,Е.К. Классификация корреляционно-иммунных и минимальных корреляционно-иммунных булевых функций от 4 и 5 переменных / Е. К. Алексеев, Е. К. Карелина–МГУ им. М.В. Ломоносова,2015 – С. 23-26. – Текст: непосредственный.

8. Функции k-значной логики. Элементарные функции. Лемма об аналоге правила де Моргана – Текст: электронный // URL: https://3dstroyproekt.ru/(дата обращения 10.04.2020).

9. ФСЭК России: официальный сайт – Текст: электронный // URL http://bdu.fstec.ru/threat(дата обращения 11.04.2020).

10. Sokolov,A.V. Correlation immunity of three – valued logic functions/ A.V. Sokolov, O.N. Zhdanov – Odessa, National Polytechnic University – С. 187-188.–Текст: непосредственный.

11. Соколов, А.В. Криптографические конструкции на основе функций многозначной логики /А.В.Соколов, О.Н.Жданов – Одесса, СибГАУ им. М.Ф. Решетнева – Текст: непосредственный.