

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт прикладной математики и компьютерных наук
Кафедра компьютерной безопасности

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
канд. техн. наук, доцент


подпись В.Н. Тренькаев
« 23 » января 2023 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА
(ДИПЛОМНАЯ РАБОТА)

АНАЛИЗ КРИПТОСИСТЕМЫ НА БУЛЕВЫХ ФУНКЦИЯХ

по специальности 10.05.01 Компьютерная безопасность,
специализация (профиль) «Анализ безопасности компьютерных систем»

Кандинский Алексей Вадимович

Научный руководитель ВКР
канд. физ.-мат. наук, доцент


подпись И.А. Панкратова
« 23 » января 2023 г.

Автор работы
студент группы № 931724


подпись А.В. Кандинский
« 23 » января 2023 г.

Министерство науки и высшего образования Российской Федерации.
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Руководитель ООП
канд. техн. наук, доцент


подпись В.Н. Тренькаев
«27» июня 2022 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы специалиста обучающемуся
Кандинскому Алексею Вадимовичу

Фамилия Имя Отчество обучающегося

по специальности 10.05.01 Компьютерная безопасность, специализация (профиль)
«Анализ безопасности компьютерных систем»

1 Тема выпускной квалификационной работы

Разработка и исследование атак на асимметричный шифр на булевых функциях

2 Срок сдачи обучающимся выполненной выпускной квалификационной работы:

а) в учебный офис / деканат – 16 января 2023 г. б) в ГЭК – 27 января 2023 г.

3 Исходные данные к работе:

Объект исследования – Асимметричный шифр на булевых функциях

Предмет исследования – Атаки на шифр

Цель исследования – Анализ атак на шифр

Задачи:

Разработать, реализовать и исследовать алгоритмы атак с известным и с выбираемым открытым текстом на асимметричный шифр на булевых функциях с двухэлементными и трёхэлементными ключами.

Методы исследования:

Теоретический и экспериментальный.

Организация или отрасль, по тематике которой выполняется работа, –

Лаборатория компьютерной криптографии ТГУ.

4 Краткое содержание работы

Описание асимметричного шифра на булевых функциях, описание алгоритмов атак на шифр, результаты исследований разработанных алгоритмов атак.

Руководитель выпускной квалификационной работы

зав. лаб. компьютерной криптографии

должность, место работы


подпись

/ И.А.Панкратова
И.О. Фамилия

Задание принял к исполнению

студент группы 931724

должность, место работы


подпись

/ А.В.Кандинский
И.О. Фамилия

АННОТАЦИЯ

Дипломная работа содержит 30 страниц, 3 рисунка, 16 таблиц, 3 источника литературы.

АСИММЕТРИЧНЫЙ ШИФР НА БУЛЕВЫХ ФУНКЦИЯХ, КРИПТОАНАЛИЗ

Актуальность:

В настоящее время активно ведутся разработки в сфере квантовых компьютеров, что заставляет задуматься о проблемах уязвимости множества современных шифров с открытым ключом к атакам с использованием квантового компьютера. Для решения этой проблемы стоит рассматривать шифры, стойкость которых основана на задачах, отличных от задачи дискретного логарифмирования и задачи факторизации целых чисел.

Объекты исследования: асимметричный шифр на булевых функциях, атаки на шифр с двухэлементными и трёхэлементными ключами.

Цель работы: разработка, реализация и исследование атак на асимметричный шифр на булевых функциях.

Задачи:

Разработать, реализовать и исследовать алгоритмы атак с известным и с выбираемым открытым текстом на асимметричный шифр на булевых функциях для случаев с двух и трёхэлементными ключевыми параметрами.

Методы исследования: теоретический (с использованием теории булевых функций, комбинаторики и теории вероятностей) и экспериментальный (на базе ЭВМ).

Результаты:

Разработаны, реализованы и исследованы алгоритмы атак с известным открытым текстом для следующих ключевых параметров: $\{\sigma_1, \sigma_2\}$, $\{\pi_1, \pi_2, \sigma_1\}$, $\{\pi_1, \pi_2, \sigma_2\}$. Также были разработаны два алгоритма атаки с выбираемым открытым текстом для ключевых параметров $\{\pi_1, \pi_2\}$.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	5
1 Асимметричный шифр на булевых функциях	6
1.1 Определения.....	6
1.2 Описание шифра	7
1.3 Основные предположения при атаках на шифр.....	8
2 Атаки на шифр с двухэлементным ключевым параметром	9
2.1 Атака с известным открытым текстом на ключ $J = \{\sigma_1, \sigma_2\}$	9
2.2 Атаки на ключ $J = \{\pi_1, \pi_2\}$	10
2.2.1 Атака с известным открытым текстом.....	10
2.2.2 Атака с выбираемым открытым текстом	12
3 Атаки на шифр с трёхэлементным ключевым параметром	20
3.1 Атака с известным открытым текстом на ключ $J = \{\pi_1, \pi_2, \sigma_1\}$	20
3.2 Атака с известным открытым текстом на ключ $J = \{\pi_1, \pi_2, \sigma_2\}$	22
3.3 Исследование атак	23
ЗАКЛЮЧЕНИЕ.....	29
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ.....	30

ВВЕДЕНИЕ

В настоящее время большое количество классических шифров с открытым ключом основано на проблемах дискретного логарифмирования, а значит, уязвимо к квантовым атакам. Криптосистемы, основой стойкости которых является сложность решения систем нелинейных уравнений над конечным полем, считаются предположительно стойкими к квантовым атакам. К классу таких криптосистем относятся криптосистемы с функциональными ключами, построенные на основе векторных булевых функций. Опираясь на эти факты, Агибаловым Г.П. был предложен асимметричный шифр, в основе которого лежит алгебра обратимых векторных булевых функций, а также операции инверсии и перестановки координат над их входными и выходными параметрами [1].

В данной работе рассматриваются вариации асимметричного шифра на булевых функциях с двухэлементными и трёхэлементными ключами, разрабатываются, реализуются и исследуются алгоритмы атак с известным и с выбираемым открытым текстом на эти вариации.

1 Асимметричный шифр на булевых функциях

1.1 Определения

Определение 1. Векторная булева функция – функция $F: Z_2^n \rightarrow Z_2^m$, где $F = (f_1 f_2 \dots f_m)$, $f_i: Z_2^n \rightarrow Z_2, i = 1, 2, \dots, m$, - координатные функции.

Определение 2. Операция перестановки – перестановка $\pi = (i_1 i_2 \dots i_n) \in S_n$, где S_n – множество всех перестановок длины n , результатом воздействия которой на произвольное слово $w = w_1 w_2 \dots w_n$ является слово $\pi(w) = w_{i_1} w_{i_2} \dots w_{i_n}$.

Определение 3. Операция инверсии – булев вектор $\sigma = b_1 b_2 \dots b_n \in Z_2^n$, результатом воздействия которого на булев вектор $\alpha = a_1 a_2 \dots a_n$ является булев вектор $\alpha^\sigma = a_1^{b_1} a_2^{b_2} \dots a_n^{b_n}$, где для $a, b \in Z_2$ выполняется

$$a^b = \begin{cases} a, & \text{если } b = 0, \\ \neg a, & \text{если } b = 1. \end{cases}$$

Договоримся обозначать операцию инверсии σ над булевым вектором α следующим образом:

$$\alpha^\sigma = \alpha \oplus \sigma.$$

Определение 4. Пусть $\pi \in S_n$, A, B – булевы матрицы размера $m \times n$, A_i, B_i , $i = 1, \dots, m$, - их строки, $A^{(j)}, B^{(j)}, j = 1, \dots, n$, - вектор-столбцы, причём $B^{(j)} = A^{(\pi(j))}$, $j = 1, \dots, n$ (обозначим $B = \pi(A)$).

Построим матрицу $D = \|d_{jk}\|$ размера $n \times n$ так [2]:

$$d_{jk} = \bigwedge_{i=1}^m a_{ik}^{b_{ij}}, j, k = 1, \dots, n,$$

Или через покомпонентную конъюнкцию строк:

$$D_j = \bigwedge_{i=1}^m A_i^{b_{ij}}, j = 1, \dots, n.$$

Условимся обозначать $D = T(A, B)$.

Если в матрице A все столбцы различны, то существует единственная перестановка π со свойством $B = \pi(A)$. Тогда $D = T(A, B)$ - матрица перестановки (т.е. $B = AD^T$) [2].

Проверить, является ли матрица D матрицей перестановок, можно с помощью алгоритма [3]:

1. Построим массив N мощностью 2^n , где n – длина строки в D .
2. Для $j = 0, \dots, n - 1$ выполняем: $N[D_j] := 0$.
3. Для $j = 0, \dots, n - 1$ выполняем: $N[D_j] := N[d_j] + 1$.
4. Для $j = 0, \dots, n - 1$: если $N[D_j] \neq w(D_j)$, то $r := 0$ и выход.
5. $r := 1$ и выход.

Если матрица D является матрицей перестановок, то $r = 1$, иначе $r = 0$.

1.2 Описание шифра

Асимметричный шифр на булевых функциях (ACBF – Asymmetric Cryptosystem on Boolean Functions) – асимметричная криптосистема, основанная на сложности обращения большой обратимой векторной булевой функции [1].

Асимметричный шифр на булевых функциях – тройка $C = (X, K, Y)$, $X \subseteq Z_2^n$ - множество открытых текстов, $Y \subseteq Z_2^n$ - множество шифртекстов, $K = K_1 \times K_2$ – множество ключей, где $K_1 \subseteq K_n(g) = \{f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))\}; \sigma_1, \sigma_2 \in Z_2^n; \pi_1, \pi_2 \in S_n\}$ – множество открытых ключей, $K_2 = \{f^{-1}: f \in K_1\}$ - множество закрытых ключей [1].

Открытым ключом является функция $f: Z_2^n \rightarrow Z_2^n$, а закрытым ключом - функция f^{-1} . Шифрование и расшифрование происходит следующим образом: $y = f(x)$; $x = f^{-1}(y)$.

Функция f имеет следующий вид:

$$f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))),$$

где $\sigma_1, \sigma_2 \in Z_2^n$ – операции инверсии, $\pi_1, \pi_2 \in S_n$ – операции перестановки, $g: Z_2^n \rightarrow Z_2^n$ – обратимая n -мерная векторная булева функция $g = (g_1 g_2 \dots g_n)$, называемая порождающей функцией криптосистемы.

Ключевыми параметрами асимметричного шифра на булевых функциях являются элементы любого непустого подмножества $J \subseteq \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$, то есть всего 15 различных вариантов. При этом операции из множества $\{\pi_1, \pi_2, \sigma_1, \sigma_2\} \setminus J$ определяются как тождественные.

1.3 Основные предположения при атаках на шифр

Будем рассматривать атаки на асимметричный шифр на булевых функциях с известным и с выбираемым открытым текстом, используя следующие предположения:

1. Для любого $x \in Z_2^n$ злоумышленник способен вычислить $g(x)$ и $g^{-1}(x)$.
2. Злоумышленник обладает информацией о том, какие операции из $\{\pi_1, \pi_2, \sigma_1, \sigma_2\}$ задействованы в функции f , но не знает их конкретных значений. Цель злоумышленника – вычислить эти значения.
3. Злоумышленник способен вычислить $f(x)$ для любого $x \in Z_2^n$ при атаке с выбираемым открытым текстом.

Целью атаки является определение значений параметров, входящих в J . При атаке с известным открытым текстом атакующий имеет набор пар открытых текстов и соответствующих им шифртекстов. При атаке с выбираемым открытым текстом атакующий имеет возможность выбирать открытые тексты и вычислять соответствующие им шифртексты.

2 Атаки на шифр с двухэлементным ключевым параметром

В данной работе для рассмотрения были выбраны подмножества ключевых параметров $J = \{\sigma_1, \sigma_2\}$, так как атаки с известным открытым текстом на оставшиеся двухэлементные подмножества были рассмотрены в работах [2,3], и $J = \{\pi_1, \pi_2\}$, так как атаки с выбираемым открытым текстом на оставшиеся двухэлементные подмножества были рассмотрены в работе [2].

2.1 Атака с известным открытым текстом на ключ $J = \{\sigma_1, \sigma_2\}$

При $J = \{\sigma_1, \sigma_2\}$ асимметричный шифр на булевых функциях принимает следующий вид:

$$y = f(x) = g^{\sigma_2}(x^{\sigma_1}) = g(x \oplus \sigma_1) \oplus \sigma_2.$$

Пусть дано m пар текстов (P_i, C_i) .

Атака с известным открытым текстом может быть проведена следующим образом:

1. Выбираем пару (P_1, C_1) , где P_1 – открытый текст, C_1 – шифртекст.
2. Выбираем $\sigma_1 \in Z_2^n$.
3. Вычисляем $\sigma_2 = g(P_1 \oplus \sigma_1) \oplus C_1$.
4. Проверяем пару (σ_1, σ_2) на удовлетворение следующим равенствам:

$$C_i = g(P_i \oplus \sigma_1) \oplus \sigma_2, i = 2, \dots, m. \quad (2.1)$$

Как только равенство (2.1) не выполнено, переходим на шаг 2, если оно выполнено для всех $i = 2, \dots, m$, то добавляем (σ_1, σ_2) в множество возможных ключевых пар M .

5. Повторяем шаги 2-4, пока не будут проверены все возможные значения σ_1 .

Для совершения атаки злоумышленнику придется перебрать 2^n пар (σ_1, σ_2) и потребуется минимум 2 пары (P_i, C_i) , чтобы уменьшить мощность множества подходящих пар M до менее чем 2^n , так как для одной пары (P_i, C_i) возможны все 2^n пар (σ_1, σ_2) .

Для проведения практических тестов была написана программа на языке Python, позволяющая провести атаку по заданной функции g и набору пар текстов, а также

определить среднее количество пар текстов, которое нужно проверить в шаге 4, чтобы нарушилось равенство. Текст программы представлен в [4].

В ходе проведения экспериментов были получены следующие результаты:

1. Для однозначного определения ключевой пары (σ_1, σ_2) необходимо наличие у злоумышленника минимум трёх пар (P_i, C_i) .
2. Для $n = 3$ однозначно определить ключевую пару можно в $\sim 73\%$ случаев при наличии всех восьми возможных пар (P_i, C_i) , зашифрованных на ключевой паре (σ_1, σ_2) .
3. Для $n \geq 4$ однозначно определить ключевую пару можно в более чем 85% случаев при наличии трёх пар (P_i, C_i) .

Из полученных результатов можно сделать вывод о том, что асимметричный шифр на булевых функциях при использовании в качестве ключевых параметров подмножества $J = \{\sigma_1, \sigma_2\}$ является недостаточно стойким для практического применения.

2.2 Атаки на ключ $J = \{\pi_1, \pi_2\}$

В данном разделе рассматривается эффективность улучшения атаки с известным открытым текстом на шифр при ключе $J = \{\pi_1, \pi_2\}$ [2] и предлагается алгоритм атаки с выбираемым открытым текстом для данного ключа.

При $J = \{\pi_1, \pi_2\}$ асимметричный шифр на булевых функциях принимает следующий вид:

$$y = f(x) = \pi_2(g(\pi_1(x))).$$

2.2.1 Атака с известным открытым текстом

Атака с известным открытым текстом может быть проведена следующим образом [2]:

1. Строим матрицу C со строками $C_i, i = 1, \dots, t$.
2. Перебираем $n!$ перестановок π'_1 - "кандидатов" в π_1 .
3. Для каждой π'_1 строим матрицу C' со строками $g(\pi'_1(P_i)), i = 1, \dots, t$.
4. Находим матрицу $D = T(C', C)$.
5. Если D не является матрицей перестановок, то π'_1 не может быть частью ключевой пары, иначе все пары (π_1, π_2) , где $\pi_1 = \pi'_1$ и π_2 содержится в D , удовлетворяют системе:

$$C_i = \pi_2 \left(g(\pi_1(x)) \right), i = 1, \dots, m.$$

Сложность атаки равна $O(n!)$.

Для уменьшения сложности атаки можно использовать инвариантность веса булева вектора относительно перестановки его координат, то есть рассматривать π'_1 , удовлетворяющие условиям:

$$w \left(g(\pi'_1(P_i)) \right) = w(C_i), i = 1, \dots, m.$$

Для этого на шаге 3 необходимо проверять строки матрицы C' на соответствие этим условиям и отбрасывать π'_1 при их нарушении [2].

Чтобы проверить, сколько в среднем строк матрицы C' необходимо построить, чтобы обнаружить нарушение приведенного условия, были проведены теоретические расчеты:

1. Вероятность того, что вес случайного булева вектора длины n равен k :

$$q = \frac{C_n^k}{2^n}.$$

2. Вероятность совпадения веса 2 случайных булевых векторов длины n :

$$p = \sum_{k=0}^n \left(\frac{C_n^k}{2^n} \right)^2 = \frac{1}{2^{2n}} \sum_{k=0}^n (C_n^k)^2 = \frac{C_{2n}^n}{2^{2n}}.$$

3. Математическое ожидание номера попытки, на котором произойдет нарушение условия:

$$M(a) = \frac{1}{1-p} = \frac{1}{1 - \frac{C_{2n}^n}{2^{2n}}}.$$

Результаты представлены в таблице 2.1.

Таблица 2.1 – Зависимость p и $M(a)$ от n

n	p	$M(a)$
1	0,5	2
2	0,375	1,6
3	0,3125	1,45455
4	0,27344	1,37634
5	0,24609	1,32642
6	0,22559	1,2913
7	0,20947	1,26498
8	0,19638	1,24437
9	0,18547	1,2277
10	0,1762	1,21388
11	0,16819	1,20219
12	0,16118	1,19215
13	0,15498	1,18341
14	0,14945	1,1757
15	0,14446	1,16886
16	0,13995	1,16272

Из расчётов можно сделать вывод, что с ростом n математическое ожидание номера попытки, при котором произойдет нарушение условия, стремится к 1, что совпадает с результатами практических экспериментов работы [3]. Это подтверждает эффективность предложенного улучшения атаки с известным открытым текстом.

2.2.2 Атака с выбираемым открытым текстом

Атаки с выбираемым открытым текстом на шифр с одноэлементными и некоторыми двухэлементными ключевыми параметрами были подробно рассмотрены ранее [2]. В данной работе для рассмотрения был выбран случай с двухэлементным ключевым параметром $J = \{\pi_1, \pi_2\}$.

Идея атаки состоит в том, чтобы искать перестановки π_1 и π_2 одновременно, используя инвариантность веса булева вектора относительно перестановки его координат, то есть:

$$w(x) = w(\pi_1(x));$$

$$w(y) = w(g(\pi_1(x))).$$

Будем вычислять пары $(x, y = f(x))$ и $(a, z = g(a))$ для всех векторов x и a веса l . Если $w(y) = w(z)$, то пары (x, a) и (z, y) могут быть включены в матрицы для поиска π_1 и

π_2 соответственно. Условие $w(y) = w(z)$ может выполняться для нескольких пар $(a, z = g(a))$ сразу, что позволяет предложить различные подходы к атаке:

1. Включать в матрицы пары (x, a) и (z, y) , только если условие выполнено один раз.
2. Копировать матрицы и добавлять в каждую копию по одной из подходящих пар, если условие выполнено больше одного раза.

Рационально рассматривать вектора веса $l = 1$ и $l = n - 1$, так как для каждого из этих случаев существует всего n векторов такого веса.

Атака 1 с выбираемым открытым текстом может быть проведена следующим образом:

1. Берём 2 пары текстов $(P, C) (0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$.
2. Строим матрицы C со строками $C_i, i = 1, 2, C'$ со строками $C'_i = g(P_i), i = 1, 2$. Фиксируем $l = 1$.
3. Вычисляем пары $(a, g(a))$ для всех a таких, что $w(a) = l$. Создаём массивы W_k , $k = 0, \dots, n$, содержащие все пары $(a, g(a))$, где $w(g(a)) = k$.
4. Выбираем пару (P_i, C_i) такую, что $w(P_i) = l$. Если $w(C_i) = k$ и W_k содержит только одну пару $(a, g(a))$, то добавляем строки P_i в матрицу P , a в матрицу P' , $g(a)$ в матрицу C' , C_i в матрицу C и повторяем Шаг 4, пока все возможные P_i не перебраны.
5. Вычисляем $D_1 = T(P, P'), D_2 = T(C', C)$ и извлекаем из них все возможные кандидаты в π_1 и π_2 соответственно. Если однозначно определили π_1 или π_2 , то переходим на шаг 6. Если ни π_1 , ни π_2 однозначно определить не удалось, то следует выполнить Шаги 3-5 для $l = n - 1$.
6. Пусть $m = \lceil \log n \rceil, t = 2^m \geq n$. Построим матрицу P'' размера $m \times t$ со строками

$$\begin{aligned} P_1'' &= (0)^{t/2} (1)^{t/2}; \\ P_2'' &= (0)^{t/4} (1)^{t/4} (0)^{t/4} (1)^{t/4}; \\ &\dots \\ P_m'' &= (01)^{t/2}, \end{aligned}$$

удалим из неё любые $(t - n)$ столбцов. Получим матрицу B , в которой все столбцы различны.

Если однозначно определили π_1 , то принимаем за открытые тексты $P_i''' = \pi_1^{-1}(g^{-1}(B_i)), i = 1, \dots, m$. Вычисляем $C'''_i = f(P_i''')$ и $C''_i =$

$= g(\pi_1(P_i'''))$, затем $D_3 = T(C'', C''')$, откуда однозначно определяем π_2 . Если однозначно определили π_2 , то принимаем за открытые тексты строки матрицы B . Вычисляем $C''_i = f(B_i)$ и $P_i''' = g^{-1}(\pi_2^{-1}(C''_i))$, $i = 1, \dots, m$, затем $D_3 = T(B, P''')$, откуда однозначно определяем π_1 .

Атака 2 с выбираемым открытым текстом может быть проведена следующим образом:

1. Берём 2 пары текстов $(P, C) (0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$.
2. Строим матрицы C со строками $C_i, i = 1, 2, C'$ со строками $C'_i = g(P_i), i = 1, 2$. Фиксируем $l = 1$.
3. Вычисляем пары $(a, g(a))$ для всех a таких, что $w(a) = l$. Создаём массивы W_k , $k = 0, \dots, n$, содержащие все пары $(a, g(a))$, где $w(g(a)) = k$.
4. Выбираем пару (P_i, C_i) такую, что $w(P_i) = l$. Если $w(C_i) = k$ и W_k содержит h пар $(a, g(a))$, то добавляем строки P_i в матрицу P , C_i в матрицу C , а матрицы P' и C' копируем $h - 1$ раз, добавляя a в матрицы P' , $g(a)$ в матрицы C' . Если a уже в матрице P' или $g(a)$ в матрице C' , то удаляем эти P' и C' . Если $w(C_i) = k$ и W_k содержит только одну пару $(a, g(a))$, то добавляем строки P_i в матрицу P , a во все матрицы P' , $g(a)$ во все матрицы C' , C_i в матрицу C . Повторяем Шаг 4, пока все возможные P_i не перебраны.
5. Вычисляем $D_1 = T(P, P'), D_2 = T(C', C)$ и проверяем, что они являются матрицами перестановок. Если D_1 или D_2 не являются матрицами перестановок, то переходим к следующей паре P' и C' . Извлекаем из D_1 и D_2 все возможные кандидаты в π_1 и π_2 соответственно и заносим в множество возможных ключей. Повторяем шаг 5, пока все возможные P' и C' не перебраны.
6. Пусть $m = \lceil \log n \rceil, t = 2^m \geq n$. Построим матрицу P'' размера $m \times t$ со строками

$$\begin{aligned} P_1'' &= (0)^{t/2} (1)^{t/2}; \\ P_2'' &= (0)^{t/4} (1)^{t/4} (0)^{t/4} (1)^{t/4}; \\ &\vdots \\ P_m'' &= (01)^{t/2}, \end{aligned}$$

удалим из неё любые $(t - n)$ столбцов. Получим матрицу B .

Если в паре из множества возможных ключей однозначно определена π_1 , то принимаем за открытые тексты $P_i''' = \pi_1^{-1}(g^{-1}(B_i))$, $i = 1, \dots, m$. Вычисляем

$C'''_i = f(P_i''')$ и $C''_i = g(\pi_1(P_i'''))$, затем $D_3 = T(C'', C''')$, откуда однозначно определяем π_2 . Если однозначно определена π_2 , то принимаем за открытые тексты строки матрицы B . Вычисляем $C''_i = f(B_i)$ и $P_i''' = g^{-1}(\pi_2^{-1}(C''_i))$, $i = 1, \dots, m$, затем $D_3 = T(B, P''')$, откуда однозначно определяем π_1 .

Были поставлены следующие задачи для исследования предложенных атак:

1. Определить среднее количество пар в массивах W_k .
2. Определить вероятность однозначного определения значения ключевых параметров.
3. Определить среднее количество строк в матрице P при Атаке 1.
4. Определить среднее количество матриц P' , построенных на шаге 4 Атаки 2.

Эксперимент 1

Задача: определить среднее количество пар в массивах W_k .

Эксперимент проводился для $n = 3, \dots, 8$. Для каждого n проводилось 10000 запусков алгоритма атаки, в которых выбирались случайные набор ключевых параметров J и функция g . В качестве результата для каждого n выводилось среднее количество пар в массивах W_k . Результаты представлены в таблице 2.2.

Таблица 2.2 – Среднее количество пар в массивах W_k

$n \backslash k$	0	1	2	3	4	5	6	7	8
3	0,37	1,11	1,13	0,36	-	-	-	-	-
4	0,24	1	1,5	0,99	0,24	-	-	-	-
5	0,15	0,78	1,55	1,57	0,77	0,15	-	-	-
6	0,09	0,56	1,4	1,87	1,41	0,55	0,09	-	-
7	0,05	0,39	1,14	1,9	1,93	1,14	0,37	0,05	-
8	0,03	0,24	0,87	1,74	2,18	1,75	0,88	0,25	0,03

Из эксперимента можно сделать вывод о том, что в среднем наибольшее количество пар $(a, g(a))$ приходится на массив $W_k, k = n/2$. Также эксперимент позволяет сделать предположение об эффективности Атаки 2, так как среднее количество пар мало и копировать матрицы на шаге 4 придется не такое большое число раз.

Эксперимент 2

Задача: определить вероятность однозначно определить значения ключевых параметров в результате атак.

Было проведено 4 эксперимента:

1. Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 1 запускался 100000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводились вероятности однозначного определения π_2 после шага 5 без использования текстов веса $n - 1$, используя и не используя пары $(0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$. Результаты представлены в таблице 2.3.

Таблица 2.3 – Вероятность однозначно определить значения π_2 после шага 5 Атаки 1

Условия \ n	3	4	5	6	7	8
Без использования пар $(0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$	0,215	0,052	0,024	0,012	0,0076	0,0046
С использованием пар $(0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$	0,813	0,593	0,393	0,265	0,189	0,14

Из эксперимента можно сделать вывод, что использование пар $(0 \dots 0, y(0 \dots 0)), (1 \dots 1, y(1 \dots 1))$ увеличивает шанс однозначно определить π_2 после шага 5 Атаки 1 более чем в n раз, что подтверждает целесообразность шагов 1 и 2 Атаки 1.

2. Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 1 запускался 100000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводились вероятности однозначного определения ключевых параметров π_1 и π_2 после шага 5 без использования текстов веса $n - 1$, вероятность однозначно определить пару π_1, π_2 в результате атаки. Результаты представлены в таблице 2.4.

Таблица 2.4 – Вероятность однозначно определить значения ключевых параметров в результате Атаки 1, используя только текст веса 1

Перестановки \ n	3	4	5	6	7	8
π_1	0,428	0,139	0,0328	0,0055	0,00067	0,00003
π_2	0,814	0,59	0,3908	0,26634	0,19099	0,13772
π_1, π_2	0,814	0,599	0,3943	0,26697	0,19104	0,13772

3. Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 1 запускался 100000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводились вероятности однозначного определения ключевых параметров π_1 и π_2 после шага 5 с использованием текстов веса $n - 1$, вероятность однозначно определить пару π_1, π_2 в результате атаки. Результаты представлены в таблице 2.5.

Таблица 2.5 – Вероятность однозначно определить значения ключевых параметров в результате Атаки 1, используя текст веса 1 и $n - 1$

Перестановки $\backslash n$	3	4	5	6	7	8
π_1	0,876	0,635	0,358	0,164	0,059	0,0186
π_2	0,877	0,848	0,722	0,62	0,543	0,4893
π_1, π_2	0,927	0,878	0,754	0,636	0,549	0,4908

Из экспериментов можно сделать вывод о том, что рассмотрение векторов веса $n - 1$ увеличивает вероятность однозначно определить π_1 более чем в n раз и π_2 приблизительно в $n/2$ раз с ростом n . Также видно, что эффективность атаки сильно падает с ростом n , что позволяет сделать вывод о необходимости использования в шагах 3-5 $l = 2, n - 2, 3, n - 3$ и т.д.

4. Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 2 запускался 100000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводилась вероятность однозначного определения ключевых параметров π_1, π_2 в результате атаки. Результаты представлены в таблице 2.6.

Таблица 2.6 – Вероятность однозначно определить значения ключевых параметров в результате Атаки 2

n	3	4	5	6	7	8
π_1, π_2	0,88	0,91	0,94	0,966	0,98	0,99

Из эксперимента можно сделать вывод о том, что с ростом n Атака 2 становится значительно эффективнее Атаки 1.

Эксперимент 3

Задача: определить среднее количество строк в матрице P при Атаке 1.

Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 1 запускался 10000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводилось среднее количество строк в матрице P при использовании текстов веса 1 и использовании текстов веса 1 и $n - 1$. Результаты приведены в таблице 2.7.

Таблица 2.7 – Среднее количество строк в матрице P при Атаке 1

Условия \ n	3	4	5	6	7	8
$l = 1$	1,82	1,86	1,91	1,97	2,04	2,12
$l = 1, n - 1$	3,64	3,73	3,82	3,94	4,09	4,24

В результате эксперимента видно, что при использовании только текстов веса 1 строк в матрице P мало для однозначного определения π_1 с высокой вероятностью. Это означает, что шаги 3-4 рационально выполнять сразу для $l = 1$ и $l = n - 1$ и затем переходить на шаг 5.

Эксперимент 4

Задача: определить среднее количество матриц P' , построенных на шаге 4 Атаки 2.

Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 2 запускался 10000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводилось h - среднее количество матриц P' , построенных на шаге 4. Результаты приведены в таблице 2.8.

Таблица 2.8 – Среднее количество матриц P' , построенных на шаге 4 Атаки 2

n	3	4	5	6	7	8
h	1,71	2,98	5,59	11,24	24,7	57,1

Эксперимент показывает, что среднее количество матриц P' увеличивается примерно в 2 раза с каждым последующим n . При этом в процессе атаки придется хранить h матриц размера $n \times n$, что при достаточно большом n делает атаку затратной по памяти.

В результате эксперимента можно предложить потенциально более эффективный вариант шага 4 Атаки 2:

Выбираем пару (P_i, C_i) такую, что $w(P_i) = l$. Если $w(C_i) = k$ и W_k содержит h пар $(a, g(a))$, то добавляем строки P_i в матрицу P , C_i в матрицу C , а матрицы P' и C' копируем $h - 1$ раз, добавляя a в матрицы P' , $g(a)$ в матрицы C' . Если a уже в матрице P' или $g(a)$

в матрице C' , то удаляем эти P' и C' . Если $D_1 = T(P, P')$ или $D_2 = T(C', C)$ не является матрицей перестановок, то удаляем эти P' и C' . Если $w(C_i) = k$ и W_k содержит только одну пару $(a, g(a))$, то добавляем строки P_i в матрицу P , a во все матрицы P' , $g(a)$ во все матрицы C' , C_i в матрицу C . Повторяем Шаг 4, пока все возможные P_i не перебраны.

Эксперимент 5

Задача: определить сколько пар матриц P', C' будет оставаться после каждой итерации улучшенного шага 4 Атаки 2.

Эксперимент проводился для $n = 3, \dots, 8$. Алгоритм Атаки 2 запускался 100000 раз, где случайно выбирались набор ключевых параметров J и функция g . В результате для каждого n выводилось h - среднее количество пар матриц P', C' , построенных на i -ой итерации шага 4. Результаты приведены в таблице 2.9.

Таблица 2.9 – Среднее количество пар P', C' на k -ой итерации улучшенного шага 4 Атаки 2

$n \backslash k$	1	2	3	4	5	6	7	8
3	1,17	1,22	1,18	-	-	-	-	-
4	1,19	1,24	1,21	1,14	-	-	-	-
5	1,2	1,25	1,2	1,14	1,09	-	-	-
6	1,2	1,23	1,18	1,12	1,07	1,04	-	-
7	1,2	1,21	1,16	1,1	1,06	1,03	1,02	-
8	1,19	1,19	1,13	1,08	1,04	1,02	1,01	1,009

Исходя из результатов эксперимента, можно сделать вывод о том, что использование предложенного улучшения для шага 4 Атаки 2 позволяет хранить в среднем во время работы программы менее 2 пар матриц.

Текст программы представлен в [4].

3 Атаки на шифр с трёхэлементным ключевым параметром

Разработка атак была начата с рассмотрения случаев, в которых один из ключевых параметров перебирается, а на оставшиеся два ключевых параметра проводится атака для случая с двухэлементными ключевыми параметрами. Атаки на шифр с двухэлементными ключевыми параметрами были подробно рассмотрены ранее [2,3].

Для всех атак были получены оценки сложности, основываясь на результатах работы [2]:

1. $J = \{\pi_1, \pi_2, \sigma_1\}, y = \pi_2 \left(g(\pi_1(x^{\sigma_1})) \right) = \pi_2 \left(g(\pi_1(x \oplus \sigma_1)) \right).$

a. Перебор π_1 .

i. Сложность - $n! C_n^{n/2}$.

b. Перебор π_2 .

i. Сложность - $n! n \log n$.

c. Перебор σ_1 .

i. Сложность - $n! 2^n$.

2. $J = \{\pi_1, \pi_2, \sigma_2\}, y = \pi_2 \left(g^{\sigma_2}(\pi_1(x)) \right) = \pi_2 \left(g(\pi_1(x)) \oplus \sigma_2 \right).$

a. Перебор π_1 .

i. Сложность - $n! n \log n$.

b. Перебор π_2 .

i. Сложность - $n! C_n^{n/2}$.

c. Перебор σ_2 .

i. Сложность - $n! 2^n$.

Для рассмотрения были выбраны самые эффективные по сложности атаки:

1. Перебор по π_2 для случая $J = \{\pi_1, \pi_2, \sigma_1\}$.

2. Перебор по π_1 для случая $J = \{\pi_1, \pi_2, \sigma_2\}$.

3.1 Атака с известным открытым текстом на ключ $J = \{\pi_1, \pi_2, \sigma_1\}$

При $J = \{\pi_1, \pi_2, \sigma_1\}$ асимметричный шифр на булевых функциях принимает следующий вид:

$$y = f(x) = \pi_2 \left(g(\pi_1(x^{\sigma_1})) \right) = \pi_2 \left(g(\pi_1(x \oplus \sigma_1)) \right).$$

Пусть имеется $m + 1$ пар открытых текстов и шифртекстов вида (P_i, C_i) , $i = 1, \dots, m + 1$.

Идея атаки состоит в том, чтобы перебрать $n!$ кандидатов в π_2 , для каждого из которых необходимо провести атаку на подмножество (π_1, σ_1) сложностью $n \log n$ [2]. Для совершения атаки необходимо иметь минимум 2 пары текстов (P_i, C_i) .

Атака с известным открытым текстом может быть проведена следующим образом:

1. Строим матрицу $P_{\oplus}$ со строками $P_{\oplus_i} = P_i \oplus P_{m+1}, i = 1, \dots, m$.
2. Фиксируем π_2 . Если все возможные π_2 перебраны, то конец .
3. Строим матрицу $P_{\oplus}'$ со строками $P_{\oplus'_i} = g^{-1}(\pi_2^{-1}(C_i)) \oplus g^{-1}(\pi_2^{-1}(C_{m+1})), i = 1, \dots, m$.
4. Строим матрицу $D = T(P_{\oplus}, P_{\oplus}')$.
5. Если D не является матрицей перестановок, то переходим на Шаг 2.
6. Находим все перестановки π_1 , содержащиеся в D .
7. Вычисляем $\sigma_1 = P_{m+1} \oplus \pi_1^{-1}(g^{-1}(\pi_2^{-1}(C_{m+1})))$ для всех перестановок из Шага 6 и заносим полученные тройки (π_1, π_2, σ_1) в список потенциальных наборов ключевых параметров. Переходим на Шаг 2.

Исходя из результатов работ об атаках на двухэлементные подмножества [3], можно сделать предположение о том, что построение матриц $P_{\oplus}'$ на Шаге 3 можно осуществлять построчно с проверкой построенных i -ых строк на удовлетворение условию:

$$w(P_{\oplus'_i}) = w(P_{\oplus_i}). \quad (3.1)$$

Как только условие нарушается, можно сделать вывод о том, что матрица D не является матрицей перестановок, и переходить на Шаг 2. Такой подход может дать существенное ускорение времени выполнения атаки, если средний номер строки, при котором условие нарушается, достаточно мал. Исходя из этого, можно предложить потенциально более эффективный вариант атаки.

Второй вариант атаки на случай $J = \{\pi_1, \pi_2, \sigma_1\}$:

1. Строим матрицу $P_{\oplus}$ со строками $P_{\oplus_i} = P_i \oplus P_{m+1}, i = 1, \dots, m$ и массив $P_{\oplus w}$, где $P_{\oplus w_i} = w(P_{\oplus_i}), i = 1, \dots, m$.
2. Фиксируем π_2 . Если все возможные π_2 перебраны, то конец .

3. Построчно строим матрицу $P_{\oplus'}$ со строками $P_{\oplus'_i} = g^{-1}(\pi_2^{-1}(C_i)) \oplus \oplus g^{-1}(\pi_2^{-1}(C_{m+1})), i = 1, \dots, m$. Если $w(P_{\oplus'_i}) \neq P_{\oplus w_i}$, то переходим на Шаг 2.
4. Строим матрицу $D = T(P_{\oplus}, P'_{\oplus})$.
5. Если D не является матрицей перестановок, то переходим на Шаг 2.
6. Находим все перестановки π_1 , содержащиеся в D .
7. Вычисляем $\sigma_1 = P_{m+1} \oplus \pi_1^{-1}(g^{-1}(\pi_2^{-1}(C_{m+1})))$ для всех перестановок из Шага 6 и заносим полученные тройки (π_1, π_2, σ_1) в список потенциальных наборов ключевых параметров. Переходим на Шаг 2.

3.2 Атака с известным открытым текстом на ключ $J = \{\pi_1, \pi_2, \sigma_2\}$

Случай $J = \{\pi_1, \pi_2, \sigma_2\}$.

При $J = \{\pi_1, \pi_2, \sigma_2\}$ асимметричный шифр на булевых функциях принимает следующий вид:

$$y = f(x) = \pi_2(g^{\sigma_2}(\pi_1(x))) = \pi_2(g(\pi_1(x)) \oplus \sigma_2).$$

Пусть имеется $m + 1$ пар открытых текстов и шифртекстов вида (P_i, C_i) , $i = 1, \dots, m + 1$.

Идея атаки состоит в том, чтобы перебрать $n!$ кандидатов в π_1 , для каждого из которых необходимо провести атаку на подмножество $\{\pi_2, \sigma_2\}$ сложностью $n \log n$ [2]. Для совершения атаки необходимо иметь минимум 2 пары текстов (P_i, C_i) .

Атака с известным открытым текстом может быть проведена следующим образом:

1. Строим матрицу $C_{\oplus}$ со строками $C_{\oplus_i} = C_i \oplus C_{m+1}, i = 1, \dots, m$.
2. Фиксируем π_1 . Если все возможные π_1 перебраны, то конец.
3. Строим матрицу $C_{\oplus'}$ со строками $C_{\oplus'_i} = g(\pi_1(P_i)) \oplus g(\pi_1(P_{m+1})), i = 1, \dots, m$.
4. Строим матрицу $D = T(C'_{\oplus}, C_{\oplus})$.
5. Если D не является матрицей перестановок, то переходим на Шаг 2.
6. Находим все перестановки π_2 , содержащиеся в D .
7. Вычисляем $\sigma_2 = \pi_2^{-1}(C_{m+1}) \oplus g(\pi_1(P_{m+1}))$ для всех перестановок из Шага 6 и заносим полученные тройки (π_1, π_2, σ_2) в список потенциальных наборов ключевых параметров. Переходим на Шаг 2.

Исходя из результатов работ об атаках на двухэлементные подмножества[3], можно сделать предположение о том, что построение матриц $C_{\oplus'}$ на Шаге 3 можно осуществлять построчно с проверкой построенных i -ых строк на удовлетворение условию:

$$w(C_{\oplus'_i}) = w(C_{\oplus_i}). \quad (3.2)$$

Как только условие нарушается, можно сделать вывод о том, что матрица D не является матрицей перестановок, и переходить на Шаг 2. Такой подход может дать существенное ускорение времени выполнения атаки, если средний номер строки, при котором условие нарушается, достаточно мал. Исходя из этого, можно предложить потенциально более эффективный вариант атаки.

Второй вариант атаки на случай $J = \{\pi_1, \pi_2, \sigma_2\}$:

1. Строим матрицу $C_{\oplus}$ со строками $C_{\oplus_i} = C_i \oplus C_{m+1}, i = 1, \dots, m$ и массив $C_{\oplus w}$, где $C_{\oplus w_i} = w(C_{\oplus_i}), i = 1, \dots, m$.
2. Фиксируем π_1 . Если все возможные π_1 перебраны, то конец.
3. Построчно строим матрицу $C_{\oplus'}$ со строками $C_{\oplus'_i} = g(\pi_1(P_i)) \oplus g(\pi_1(P_{m+1})), i = 1, \dots, m$. Если $w(C_{\oplus'_i}) \neq C_{\oplus w_i}$, то переходим на Шаг 2.
4. Строим матрицу $D = T(C'_{\oplus}, C_{\oplus})$.
5. Если D не является матрицей перестановок, то переходим на Шаг 2.
6. Находим все перестановки π_2 , содержащиеся в D .
7. Вычисляем $\sigma_2 = \pi_2^{-1}(C_{m+1}) \oplus g(\pi_1(P_{m+1}))$ для всех перестановок из Шага 6 и заносим полученные тройки (π_1, π_2, σ_2) в список потенциальных наборов ключевых параметров. Переходим на Шаг 2.

3.3 Исследование атак

Эксперимент 1

Задача: проверить количество строк, на котором происходит нарушение условия равенства весов строк матриц.

Эксперимент проводился для $n = 2, \dots, 10$. Для каждого n 100 раз выбиралось случайное m в отрезке $[2, \dots, 2^n]$ и проводилось 100 запусков алгоритма атаки, в которых

выбирались случайные набор ключевых параметров J , функция g и пары текстов (P, C) . В качестве результата для каждого n выводилось среднее количество строк, на котором нарушается условие. Результаты приведены в таблице 3.1.

Таблица 3.1 – Среднее количество строк, при котором нарушается равенство весов

n	2	3	4	5	6	7	8	9	10
Количество строк	1,8	2	1,7	1,6	1,4	1,27	1,25	1,23	1,24

Из эксперимента можно сделать вывод о том, что с ростом n в среднем придется проверить не более 1 строки, чтобы обнаружить нарушение условий (3.1) и (3.2). Этот вывод можно сравнить с выводами об эффективности проверки весов строк матриц для случая $J = \{\pi_1, \pi_2\}[3]$, что показывает, что добавление в ключ третьего элемента σ_1 или σ_2 не влияет существенно на средний номер строки, при котором нарушается условие равенства весов строк. Этот эксперимент подтверждает потенциальную эффективность предложенных вторых вариантов атак.

Эксперимент 2

Задача: вычислить количество пар текстов, необходимое для однозначного определения ключа.

Было проведено 2 эксперимента:

1. Эксперимент проводился для $n = 3, \dots, 9$ и $m = 3, \dots, 16$. Второй алгоритм атаки запускался для каждой пары n, m 10000 раз, где случайно выбирались набор ключевых параметров J , функция g и пары текстов (P, C) . В результате для каждого n выводилось m , при котором вероятность однозначного определения набора ключевых параметров J была выше 90%. Результаты эксперимента приведены в таблице 3.2.

Таблица 3.2 – Количество пар текстов для однозначного определения ключа с вероятностью выше 90%

	n	3	4	5	6	7	8	9
$J = \{\pi_1, \pi_2, \sigma_1\}$	Количество текстов	6	6	8	9	9	10	10
$J = \{\pi_1, \pi_2, \sigma_2\}$	Количество текстов	6	6	8	9	9	10	10

2. Эксперимент проводился для $n = 3, \dots, 9$ и $m = 3, \dots, 16$. Второй алгоритм атаки запускался для каждой пары n, m 10000 раз, где случайно выбирались набор

ключевых параметров J , функция g и пары текстов (P, C) . В результате для каждого n выводилось m , при котором вероятность однозначного определения набора ключевых параметров J была выше 99,95%. Результаты приведены в таблице 3.3.

Таблица 3.3 – Количество пар текстов для однозначного определения ключа с вероятностью выше 99,95%

	n	4	5	6	7	8	9
$J = \{\pi_1, \pi_2, \sigma_1\}$	Количество текстов	10	13	16	16	17	17
$J = \{\pi_1, \pi_2, \sigma_2\}$	Количество текстов	10	13	15	16	16	16

Эксперимент 3

Задача: сравнить среднее время выполнения первого и второго варианта атаки.

Эксперимент проводился при одинаковых данных (набор ключевых параметров J , функция g , пары текстов (P, C)). Алгоритмы атак запускались по 10000 раз для $n < 7$, 1000 раз для $n < 9$, 100 раз для $n = 9$, для каждого n выбиралось m из Эксперимента 2. Результаты приведены в таблицах 3.4, 3.5 и на рисунках 3.1, 3.2.

Таблица 3.4 – Сравнение времени выполнения вариантов атак для случая $J = \{\pi_1, \pi_2, \sigma_1\}$

Атака\п	3	4	5	6	7	8	9
Атака 1	0,000146	0,000637	0,00487	0,0377	0,304	3,07	31,91
Атака 2	0,00007	0,000176	0,00073	0,0043	0,031	0,273	2,6
Ускорение	2,08	3,62	6,67	8,76	9,8	11,24	12,27

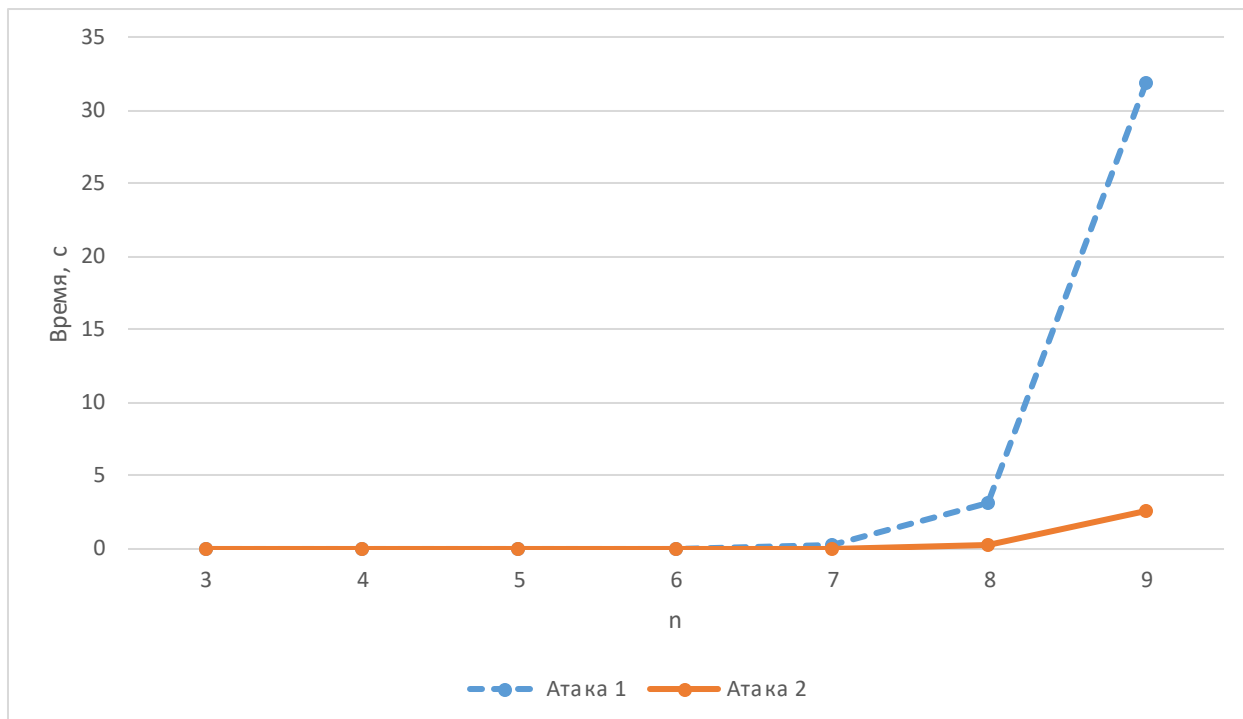


Рисунок 3.1 – Среднее время выполнения атаки для случая $J = \{\pi_1, \pi_2, \sigma_1\}$

Таблица 3.5 – Сравнение времени выполнения вариантов атак для случая $J = \{\pi_1, \pi_2, \sigma_2\}$

Атака\п	3	4	5	6	7	8	9
Атака 1	0,000143	0,000622	0,00483	0,0371	0,303	2,91	32,13
Атака 2	0,000065	0,000159	0,00064	0,0036	0,026	0,224	2,173
Ускорение	2,2	3,91	7,54	10,3	11,65	12,99	14,78

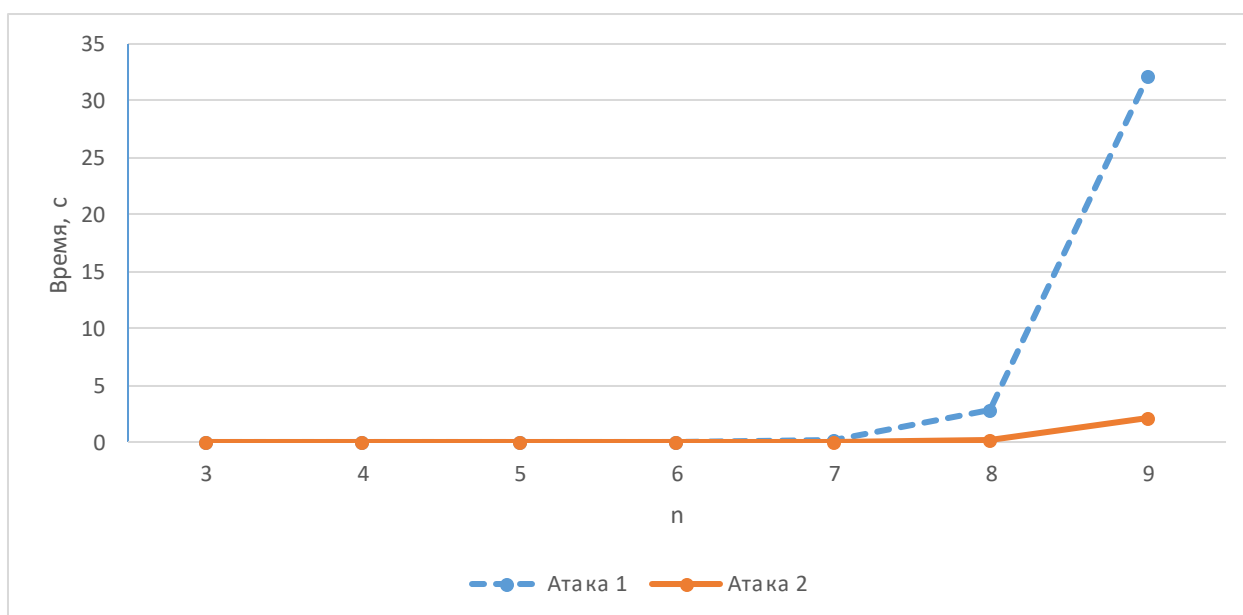


Рисунок 3.2 – Среднее время выполнения атаки для случая $J = \{\pi_1, \pi_2, \sigma_2\}$

Эксперимент 4

Задача: определить среднее время выполнения атаки для второго варианта атаки.

Алгоритм атаки запускался со случайным выбором набора ключевых параметров J , функции g и пары текстов (P, C) 10000 раз для $n < 7$, 1000 раз для $7 \leq n < 9$, 50 раз для $9 \leq n < 11$, 10 раз для $11 \leq n \leq 12$. Результаты представлены в таблицах 3.6, 3.7.

Таблица 3.6 – Среднее время выполнения второго варианта атаки в зависимости от n, t для случая $J = \{\pi_1, \pi_2, \sigma_1\}$

$n \backslash m$	2	3	4	5	6	7	8
3	0,000091	0,000068	0,000065	0,000066	0,00007	0,000074	0,000079
4	0,0004	0,0002	0,00017	0,00017	0,00017	0,00017	0,00018
5	0,0035	0,00096	0,00075	0,00071	0,00071	0,00071	0,00071
6	0,05	0,005	0,0044	0,0042	0,0042	0,0044	0,0043
7	1,44	0,045	0,031	0,031	0,031	0,031	0,031
8	35,6	0,458	0,269	0,267	0,267	0,267	0,262
9	-	6,658	3,1	2,77	2,74	2,67	2,55
10	-	128	30,7	29,4	28,9	28,7	28,9
11	-	-	-	-	-	-	323,6
12	-	-	-	-	-	-	4108

Таблица 3.7 – Среднее время выполнения второго варианта атаки в зависимости от n, t для случая $J = \{\pi_1, \pi_2, \sigma_2\}$

$n \backslash m$	2	3	4	5	6	7	8
3	0,000092	0,000068	0,000064	0,000066	0,00007	0,000078	0,000079
4	0,00044	0,00022	0,00018	0,00017	0,00017	0,00017	0,00018
5	0,0036	0,001	0,00079	0,00075	0,00075	0,00075	0,00074
6	0,052	0,006	0,0045	0,0044	0,0043	0,0044	0,0043
7	1,44	0,0468	0,033	0,031	0,031	0,031	0,031
8	35,9	0,45	0,273	0,267	0,268	0,267	0,269
9	-	6,47	2,9	2,65	2,63	2,60	2,5
10	-	128,3	29,73	27,25	27,5	28,01	27,98
11	-	-	-	-	-	-	298,4
12	-	-	-	-	-	-	3485

Из эксперимента видно, что при $t < 4$ время атаки значительно больше, чем при других t , что, предположительно, связано с количеством перестановок, содержащихся в матрице D . Также можно сделать вывод о том, что реализацию второго варианта атаки рационально использовать при $n < 12$ и $t \geq 3$.

Так как при значениях $t > 3$ время атаки приблизительно одинаково, был проведен дополнительный эксперимент для сравнения времени выполнения второго варианта атаки для случаев $J = \{\pi_1, \pi_2, \sigma_1\}$ и $J = \{\pi_1, \pi_2, \sigma_2\}$ при $t = 8$ для $n = 3, \dots, 12$. Результат приведен на рисунке 3.3.

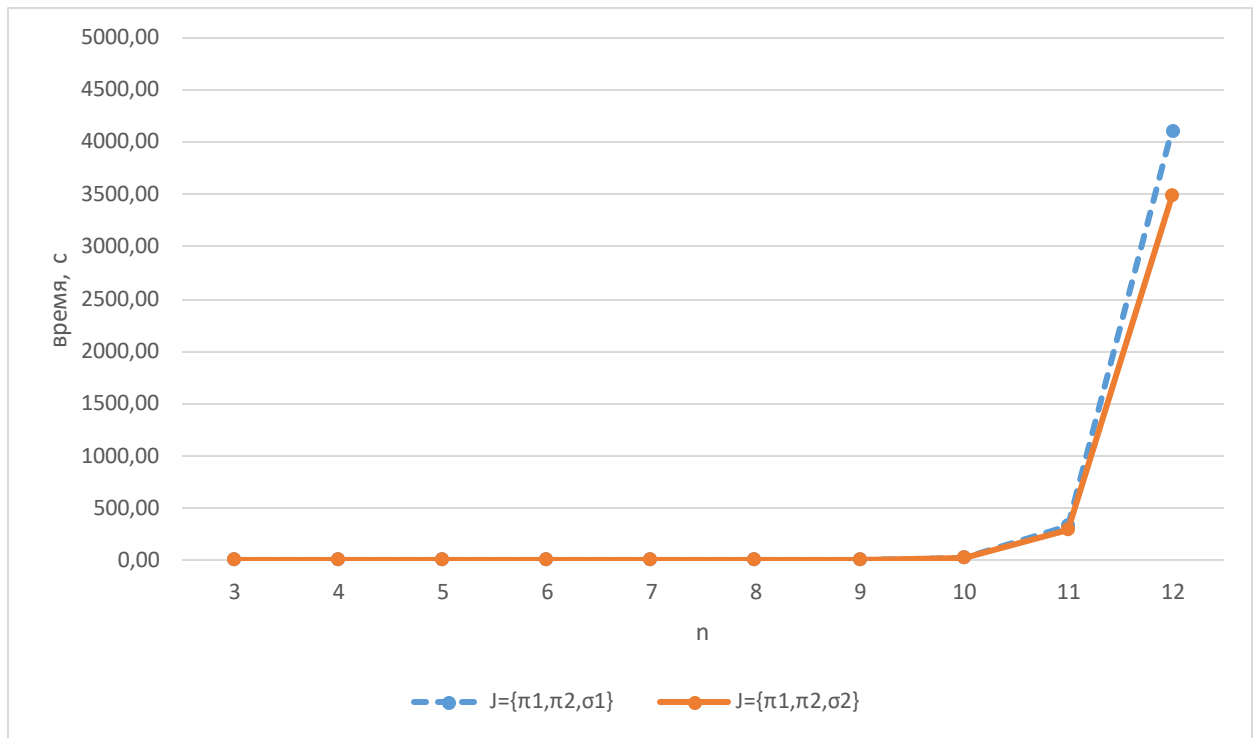


Рисунок 3.3 – Среднее время выполнения второго варианта атаки при $m = 8$

Для проведения экспериментов была написана программа на языке Python, позволяющая провести атаки по заданной функции g и набору пар текстов (P_i, C_i) , $i = 1, \dots, m$, определить средний номер строки, при котором нарушаются условия (3.1) и (3.2), измерить среднее время выполнения атаки и определить количество пар текстов (P_i, C_i) необходимых для однозначного определения ключевых параметров с заданной вероятностью.

Текст программы представлен в [4].

ЗАКЛЮЧЕНИЕ

В рамках данной работы разработаны алгоритмы атак с известным открытым текстом на асимметричный шифр на булевых функциях, в качестве ключевых параметров которого выступают двухэлементное подмножество, состоящее из двух инверсий, и трёхэлементные подмножества, состоящие из двух перестановок и инверсии. Также разработаны алгоритмы атак с выбираемым открытым текстом для случая, где в качестве ключевых параметров выступает двухэлементное подмножество, состоящее из двух перестановок.

Для каждого из разработанных алгоритмов атак написана программная реализация, на основе которой проведены исследования соответствующего алгоритма. В ходе исследований были экспериментально получены оценки количества пар текстов, необходимых для однозначного определения ключевых параметров при атаках с известным открытым текстом. Также на основе проведенных экспериментов предложены и реализованы улучшения для разработанных атак.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Agibalov G.P. and Pankratova I. A. Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. №40. С.23–33.
2. Боровкова И.В., Кондратьев В.А., Панкратова И.А. Криптоанализ асимметричного шифра на булевых функциях // Прикладная дискретная математика. 2020. №50. С.42–50.
3. Кондратьев В.А. Исследование стойкости асимметричной криптосистемы на булевых функциях: дипломная работа (проект) специалиста по направлению подготовки: 10.05.01 - Компьютерная безопасность [Электронный ресурс] – URL: <https://vital.lib.tsu.ru/vital/access/manager/Repository/vital:15773> (дата обращения: 17.12.2022).
4. Ссылка на программный код [Электронный ресурс] – URL: <https://github.com/Rollistar/ACBFAttacks/blob/main/ACBF.py> (дата обращения: 16.01.2023).

Отчет о проверке на заимствования №1



Автор: reiligan@mail.ru / ID: 4931576

Проверяющий:

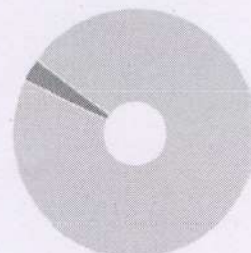
Отчет предоставлен сервисом «Антиплагиат» - <http://users.antiplagiat.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 15
Начало загрузки: 21.01.2023 08:33:17
Длительность загрузки: 00:00:01
Имя исходного файла: Диплом Кандинский
A.B. 931724.pdf
Название документа: Диплом Кандинский
A.B. 931724
Размер текста: 42 кБ
Символов в тексте: 42808
Слов в тексте: 5585
Число предложений: 212

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Начало проверки: 21.01.2023 05:33:21
Длительность проверки: 00:00:11
Комментарии: не указано
Модули поиска: Интернет Free



СОВПАДЕНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
3,35%	0%	0%	96,65%

Совпадения — доля всех найденных текстовых пересечений, за исключением тех, которые система отнесла к цитированиям, по отношению к общему объему документа.

Самоцитирования — доля фрагментов текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа, по отношению к общему объему документа.

Цитирования — доля текстовых пересечений, которые не являются авторскими, но система посчитала их использование корректным, по отношению к общему объему документа. Сюда относятся оформленные по ГОСТу цитаты; общеупотребительные выражения; фрагменты текста, найденные в источниках из коллекций нормативно-правовой документации.

Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.

Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.

Оригинальность — доля фрагментов текста проверяемого документа, не обнаруженных ни в одном источнике, по которым шла проверка, по отношению к общему объему документа.

Совпадения, самоцитирования, цитирования и оригинальность являются отдельными показателями и в сумме дают 100%, что соответствует всему тексту проверяемого документа.

Обращаем Ваше внимание, что система находит текстовые пересечения проверяемого документа с проиндексированными в системе текстовыми источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности заимствований или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

№	Доля в отчете	Доля в тексте	Источник	Актуален на	Модуль поиска	Блоков в отчете	Блоков в тексте	Комментарии
[01]	1,07%	1,64%	http://vital.lib.tsu.ru/vital/access/services/Download/vital:11008/SOURCE01 http://vital.lib.tsu.ru	24 Янв 2020	Интернет Free	14	14	
[02]	1,36%	1,36%	http://vital.lib.tsu.ru/vital/access/services/Download/vital:8664/SOURCE01 http://vital.lib.tsu.ru	24 Янв 2020	Интернет Free	10	10	
[03]	0,71%	1,03%	http://vital.lib.tsu.ru/vital/access/services/Download/vital:6890/SOURCE01 http://vital.lib.tsu.ru	07 Сен 2020	Интернет Free	2	5	

Еще источников: 3

Еще совпадений: 0,21%

С результатами ознакомлена.
Руководитель *Паш* (И. А. Панкратова)