МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Криптографические свойства булевых функций в приложении к клеточным автоматам

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Самойлова Александра Алексеевича

Научный руководитель
д. ф-м. н., профессор _____ В. А. Молчанов
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

Криптография – это совокупность идей и методов, связанных с преобразованием информации с целью ее защиты от непредусмотренных пользователей. Информация считается представленной в виде некоторого текста (сообщения), называемого открытый текст. Способ его преобразования в защищенную форму называется шифром, процесс применения шифра называется шифрованием, полученный в результате шифрования измененный текст – криптограммой. Перевод криптограммы в исходный открытый текст производится в ходе дешифрования.

В системах шифрования, основанных на переводе открытого сообщения в зашифрованное с помощью секретного ключа, особую роль играет аппарат булевых функций. Ко всем этим функциям предъявляются особые требования, которые помогают усложнить расшифровку сообщения злоумышленником.

Булевы функции играют важную роль в симметричной криптографии. Криптографическая полезность булевых функций измеряется некоторыми криптографическими характеристиками. Наиболее важными из этих свойств являются следующие: высокая алгебраическая степень, сбалансированность, высокая нелинейность, отказоустойчивость, критерии распространения более высокого порядка и отсутствие ненулевых линейных структур. Для того чтобы противостоять современным криптоаналитическим атакам (основанным на линейной аппроксимации и дифференциальных характеристиках), в основном необходимы сильно нелинейные булевы функции с хорошими критериями распространения и менее линейной структурой.

Целью данной работы является разработка анализатора криптографических свойств булевых функции, используемых в клеточных автоматах.

Решаемые задачи:

1. Разработка анализатора криптографических свойств булевых функции в приложение клеточного автомата.

2. Применить полученный анализатор для нахождения булевых функции с наилучшими криптографическими характеристиками.

3. Использовать полученные булевы функции для генерации псевдослучайно последовательности с помощью клеточного автомата и тестирование этой последовательности.

Основной целью данной работы является изучение криптографических свойств локальных функций перехода элементарных клеточных автоматов (ЭКА). Клеточные автоматы в простейшем случае представляют собой конечную совокупность элементарных ячеек, расположенных линейно в решетке и взаимодействующих на дискретном временном шаге. Состояние каждой ячейки синхронно обновляется в соответствии с булевой функцией, значениями переменных которой являются состояния соседних ячеек.

Общий объем работы – 48 страниц, из них 41 страниц – основное содержание, включая 14 рисунков и 3 таблицы, список использованных источников из 13 наименований. Приложение в работе занимает 7 страниц и содержит исходный код разработанного программного комплекса, предназначенного для анализа криптографических свойств булевых функции, используемых в клеточном автомате, на языке программирования C++.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы посвящен рассмотрению поточного шифрования на примере шифра Вернама.

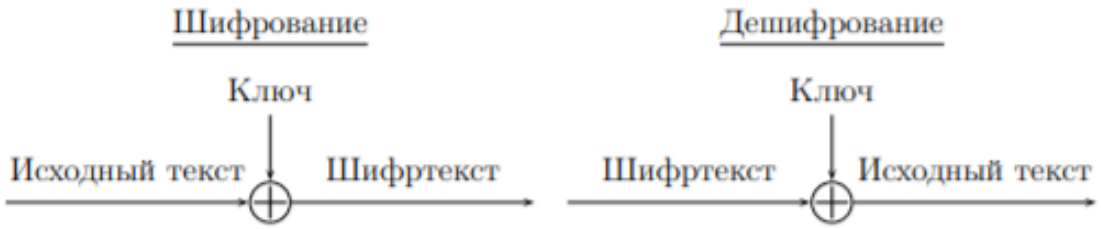

Рисунок 1 – Схема шифра Вернама

Исходный текст, ключ, шифртекст — бинарные строки одинаковой длины. Операция $\oplus$ означает побитовое сложение по модулю 2. При дешифровании схема та же, что и при шифровании, только исходный текст и шифртекст меняются местами.

Во втором разделе описаны основные принципы К. Шеннона:

1) Рассеивание — распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.

2) Усложнение — шифрование должно усложнять взаимосвязи между элементами данных, чтобы злоумышленнику было сложно получить информацию о взаимосвязи между открытым текстом, ключом и шифртекстом.

Так же в этом разделе рассмотрено устройство регистр сдвига с линейной обратной связью.

Более полувека, прошедшие с момента создания принципов Шеннона, подтвердили их значимость в криптографии. За эти годы производились различного вида атаки на криптосистемы, в связи с которыми появились основные криптографические характеристики булевых функций, некоторые из которых больше относятся к рассеиванию, другие больше к запутыванию. Все эти характеристики надо учитывать при конструировании булевых функций.

Требуется компромисс между ними, ибо булева функция не может быть оптимальна сразу по всем криптографическим показателям.

Третий раздел дипломной работы содержит описание основных математических понятий и описание криптографических характеристик булевых функций. Данный раздел содержит два подраздела, в первом из которых рассматриваются следующие начальные понятия булевых функций: булева функция, расстояние Хэмминга, теорема Жегалкина, алгебраическая нормальная форма, аффинное множество, дискретное преобразование Фурье, преобразование Уолша.

Булева функция f с n переменными — это функция от элементов векторного пространства $\mathbb{F}_2^n$, сформированного для всех двоичных векторов длины n над конечным полем $\mathbb{F}_2 = \{0,1\}$.

Вес Хэмминга вектора $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ — это число его ненулевых координат, тогда как вес Хэмминга булевой функции f с n переменными определяется как

$$\omega_H(f) = |\{x \in \mathbb{F}_2^n, \text{где } f(x) \neq 0\}|.$$

Булева функция степени 1 называется *аффинной*. Её АНФ имеет вид:

$$f(x_1, \dots, x_n) = a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n \oplus a_0,$$

где $a_0, a_1, \dots a_n \in \mathbb{F}_2$.

Во втором подразделе рассматриваются криптографические характеристики булевых функций и способы нахождения наиболее криптоустойчивых булевых функций.

Основными показателями криптографической стойкости булевых функций являются:

1) сбалансированность;

2) нелинейность;

3) корреляционный иммунитет;

4) критерий распространения (строгий лавинный критерий);

5) алгебраическая степень.

На функции, используемые в криптографии, накладывается требование сбалансированности, чтобы избежать статистических зависимостей между входными данными и выходными, которые могут использоваться в атаках на шифр. Отсутствие статистических зависимостей между входными последовательностями и выходными показывает корреляционный иммунитет нелинейной функции.

Функция f от n, переменных обладает *корреляционным иммунитетом* порядка k, если её выходная последовательность y статистически не зависит от любого подмножества размером k из входных координат $\{x_1, \dots, x_n\}$.

Функция f над полем $GF(2)$ удовлетворяет $\text{КР}(\alpha)$ – критерию распространения относительно вектора α, если функция $f(x) \oplus f(x \oplus \alpha)$ является сбалансированной.

Алгебраической степенью $deg(f)$ *функции* f называется степень самого длинного слагаемого ее АНФ.

С помощью метода треугольника Паскаля считается алгебраическая степень функции f.

Нелинейность функции f – минимальное расстояние Хэмминга N_f между функцией f и всеми афинными функциями над $GF(2)$:

$$N_f = \min\{d(f, \varphi)\},$$

где φ – множество всех аффинных функций.

Для сбалансированной функции f над $GF(2)(n \geq 3)$ нелинейность ограничена сверху значением [1]:

$$N_f = \begin{cases} 2^{n-1} - 2^{\left(\frac{n}{2}-1\right)} - 2, n = 2k \\ \left|2^{n-1} - 2^{\frac{n}{2}-1}\right|, n = 2k+1 \end{cases},$$

где |x| – максимальное четное целое, меньшее либо равное x.

В четвертом разделе работы рассматриваются основные понятия клеточного автомата, использование его в криптографии и какие клеточные автоматы бывают. Этот раздел содержит три подраздела.

Теория клеточных автоматов применяется в криптографии, как и другие разделы математики. В период 80-х – начала 90-х годов началось активное изучение приложения теории клеточных автоматов в криптографии. В последующим изучение приутихло, так как первые криптографические алгоритмы, использовавших модель клеточных автоматов, имели ряд проблем. Все эти проблемы напрямую связаны с людьми, имевшими о криптографии самое поверхностное представление. Поэтому работы по данной тематике были не компетентны.

В последнее время к этой тематике стали вновь проявлять интерес. Количество работ по данной теме значительно увеличилось. Все это объясняется самой сутью клеточных автоматов и, прежде всего, свойствами параллельности и локальности. Эти свойства дают возможность организовать параллельную обработку большого количества данных с помощью наименьшего количества вычислительного ресурса.

Первым кто стал исследовать клеточные автоматы как генераторы псевдослучайных последовательностей был С. Вольфрам. В первую очередь им были рассмотрены одномерные клеточные автоматы в качестве генераторов гаммы поточного шифрования.

В первом подразделе описываются элементарные клеточные автоматы.

Элементарные клеточные автоматы (сокращенно ЭКА) – это конечные автоматы, образованные *m* блоками памяти, называемыми ячейками, которые расположены линейно. Каждая ячейка принимает состояние из конечного множества состояний $\mathbb{F}_2$ на каждом шаге времени. Состояние i-й ячейки в момент времени *t* обозначается $s_i^t \in \mathbb{F}_2^n$ и изменяется синхронно с дискретными шагами времени в соответствии с функцией перехода *f*. Эта функция представляет собой булеву функцию с тремя переменными, переменными которой являются предыдущие состояния основной ячейки и двух ее соседних ячеек.

В настоящее время ЭКА используются в генераторе псевдослучайных последователей в пакете Wolfram Mathematica, разработанном компанией Wolfram Research.

Во втором подразделе рассматриваются двумерные клеточные автоматы.

Работ о возможности применении двумерных клеточных автоматах (ДКА) в качестве генераторов достаточно мало. Для характеристики криптографических свойств ДКА используют понятие лавинного эффекта. Это свойство показывает на сколько входные данные влияют на выходные. Это свойство играет важную роль в криптографии при исследовании блочных шифров и хэш-функций.

В третьем подразделе описаны обобщенные клеточные автоматы.

Клеточные автоматы используются во многих областях науки, например, физика, химия, и биология и т.д. С помощью них можно воспроизводить многие природные явления. В связи с тем, что клеточные автоматы имеют регулярную структуру, это ведет к снижению криптографической стойкости. Это главная причина, по которой клеточные автоматы в криптографии широкого применения не нашли. Поэтому для криптографии важен отказ от регулярной структуры, что влечен к потере клеточного автомата некоторых преимуществ.

В пятом разделе описывается сравнительный анализ булевых функций от разного количества переменных, здесь же приводятся примеры входных параметров разработанного программного комплекса, гистограммы зависимостей, статистические выводы, предположения о наилучших функциях, алгоритмы для программного комплекса.

Для создания криптографический стойких булевых функций необходимо, чтобы они имели описанные выше показатели криптографической стойкости. Очевидно, что максимизация значений этих показателей положительно влияет на криптостойкость булевой функции.

Как показали исследования явной корреляции между степенью и величиной нелинейности для сбалансированных булевых функций отсутствует. В то же время, существуют сбалансированные функции, одновременно удовлетворяющие условиям высокой степени нелинейности и максимальности значения нелинейности. Именно такие функции лучше всего подходят для использования в криптографических системах. Тем не менее, если наиболее криптостойкие функции от 3, 4, 5 переменных можно найти с помощью перебора, то для перебора функций от 6 и более переменных требуются большие компьютерные мощности. Для примера приведена гистограмма на рисунке 8 зависимостей количества булевых функций 3 переменных от криптографических свойств.

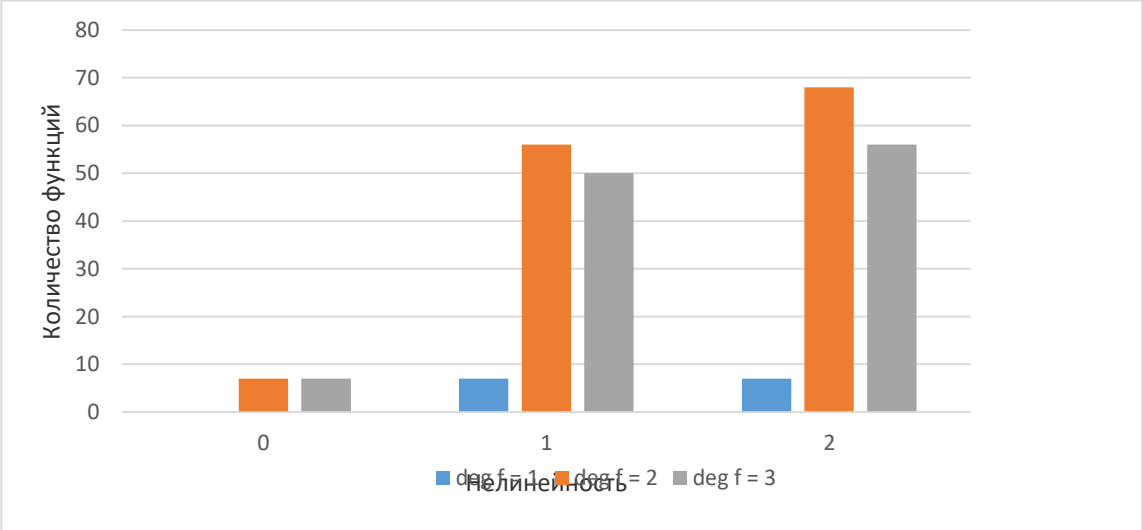

Рисунок 8 – Распределение количества булевых функций от 3 переменных значений нелинейности и степени

Можно сделать предположение, что сбалансированные функции с четным количеством переменных больше 8 будут характеризоваться схожим распределением значения нелинейности – большее количество функций будет иметь близкие к верхней границе значения нелинейности.

В шестом разделе проводиться тестирование выходных последовательностей генератора на основе клеточного автомата. Исследование выходных последовательностей разработанного генератора псевдослучайных чисел на основе примитивного клеточного автомата было проведено для

проверки свойств булевых функций и оценки их криптостойкости. Для этого к полученным последовательностям был применен набор статистических тестов NIST, результатом работы каждого из которых являются разные величины. Результаты тестирования представлены в таблице 4.

Таблица 4 – Количество пройденных тестов NIST, в зависимости от функции перехода от 3 переменных

Тесты	**f = 00110011**	**f = 11101010**	**f = 11111110**	**f = 01110100**	**f = 10001011**
Свойства	линейная, deg f = 1, сбалансир.	deg f = 2, нелин. = 1.	deg f = 3.	deg f = 2, нелин. = 2, сбалансир.	deg f = 2, нелин. = 2, сбалансир.
FT	Успешно	Неудачно	Неудачно	Успешно	Успешно
FTB	Успешно	Неудачно	Неудачно	Успешно	Успешно
RT	Успешно	Неудачно	Неудачно	Неудачно	Успешно
TLROB	Неудачно	Неудачно	Неудачно	Неудачно	Неудачно
BMRT	Неудачно	Неудачно	Неудачно	Неудачно	Успешно
DFTT	Неудачно	Неудачно	Неудачно	Неудачно	Неудачно
NTMT	Неудачно	Неудачно	Неудачно	Успешно	Успешно
OTMT	Неудачно	Неудачно	Неудачно	Успешно	Успешно
MUST	Успешно	Неудачно	Неудачно	Неудачно	Неудачно
LCT	Неудачно	Неудачно	Неудачно	Успешно	Успешно
ST	Неудачно	Неудачно	Неудачно	Неудачно	Неудачно
AET	Неудачно	Неудачно	Неудачно	Неудачно	Неудачно
CST	Успешно	Неудачно	Неудачно	Успешно	Успешно
RET	Неудачно	Неудачно	Неудачно	Неудачно	Успешно
REVT	Успешно	Неудачно	Неудачно	Успешно	Успешно

Седьмой раздел содержит описание реализованного в ходе выполнения дипломной работы программного комплекса. Программа для анализа криптографических свойств булевых функций, реализована на языке C++.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы рассмотрены важные понятия, связанные с булевыми функциями и клеточными автоматами, проведен анализ криптографических характеристик булевых функций.

В практической части работы реализована программа на языке программирования C++, имеющая возможность в зависимости от количества переменных определять булевы функции с наилучшими криптографическими характеристиками. Помимо этого, программа реализует генератор псевдослучайных последовательностей на основе клеточного автомата.

Стоит отметить, что в зависимости от выбора булевой функции в качестве функции перехода автомата, выходная последовательность проходит разное количество статистических тестов NIST.

Все поставленные в рамках данной работы задачи выполнены полностью.

Полученные результаты могут использоваться для выбора булевых функций с наиболее лучшими криптографическими характеристиками, а также в криптографии для улучшения криптостойкости шифров.