Г.1 Математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций

Рассматривается традиционная математическая модель регулярных нелинейных узлов замен с использованием совокупности булевых функций. Разрабатывается математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций. Вводятся спектральные и корреляционные преобразования недвоичных функций.

перечень ключевых слов: нелинейный узел замен, нелинейность, автокорреляция, спектральное преобразование

Постановка проблемы в общем виде

и анализ литературы

Регулярные нелинейные криптографические функции (узлы замен) симметричных шифров реализуют отображение n-битных блоков входных данных в m-битные выходные блоки: . Традиционный подход к описанию, оцениванию и разработке методов синтеза регулярных нелинейных узлов замен состоит в представлении функции F с помощью ее координатных функций, которые задаются в терминах булевой алгебры [1]. В то же время, как показано в [2, 3], построение нелинейных узлов замен с высокими показателями стойкости через итеративное формирование компонентных булевых функций является непрактичным уже при n = 6 и вычислительно недостижимым для n > 6. Это предполагает обоснование новых подходов к описанию криптографических узлов замен симметричных шифров, исследование математического аппарата оценивания основных показателей стойкости и построение вычислительно эффективных алгоритмов синтеза.

Традиционный подход к описанию нелинейных узлов замен через компонентные булевы функции

Введем основные понятия и определения математического аппарата булевой алгебры, используемые в дальнейшем при описании нелинейных узлов замен через компонентные булевы функции и оценке их криптографических свойств.

Булевой функцией от n переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов длины n в поле [4]. Обычно булевы функции представляются в алгебраической нормальной форме (АНФ), т.е. рассматриваются как сумма произведений составляющих координат:

(1)

где - уникальные двоичные константы, а суммирование и умножение производится в двоичном поле GF(2).

Поле $GF(2^n)$ состоит из 2^n векторов , :

, , …, , ,

где – векторное пространство над .

Таблицей истинности функции f называется (0,1)-последовательность, определенная как [5]:

.

Последовательностью функции f, обозначаемой $\hat{f}$, называется (1,-1)-последовательность, определенная как [5]:

.

Рассмотрим криптографические свойства функций, реализующих отображения из в , где . Пусть есть множество таких функций, а есть множество булевых функций от n переменных, то есть функций, реализующих отображения из в . Тогда любую функцию можно рассматривать как состоящую из m булевых функций от n переменных, т.е. m-выходных координатных функций из .

В более общем представлении, компонентная функция является ненулевой линейной комбинацией ее координатных функций из .

Таким образом, функцию запишем через множество

,

где .

Алгебраическая степень f [5], обозначаемая , определяется как максимальная степень многочлена представленного в АНФ.

Важные свойства булевых функций изучаются с использованием преобразования Уолша-Адамара.

Преобразование Уолша-Адамара функции есть вещественная функция [5]:

, (2)

где скалярное произведение векторов x и w определяется как

.

Булева функция f сбалансирована, если вероятности событий и равны. Используя преобразование Уолша-Адамара, условие сбалансированности функции f запишем в виде .

Расстояние по Хеммингу между двумя функциями f и g из определяется как:

. (3)

Нелинейность функции определяется как [5]:

, (4)

где - множество всех аффинных функций от n переменных,

. (5)

С использованием преобразования Уолша-Адамара нелинейность функции f может быть получена следующим образом:

. (6)

Взаимосвязь показателя нелинейности функции с преобразованием Уолша-Адамара и вывод формулы (6) легко понять, представив выражение (2) в виде матричного умножения последовательности функции , на матрицу Уолша-Адамара порядка :

(последовательность функции в данном выражении и далее по тексту представляется в виде вектора-строки, образованной элементами этой последовательности).

Итеративное правило построения матрицы задается следующим выражением:

,

, .

Каждая строка матрицы Уолша-Адамара соответствует последовательности некоторой аффинной функции из с в общем представлении (5). Строго говоря, полное множество последовательностей всех аффинных функций с упорядочены по строкам (столбцам) матрицы Уолша-Адамара естественным образом:

,

где - i-я аффинная функция, из упорядоченного подмножества аффинных функций с в (5).

Другими словами, последовательность i-й аффинной функции из соответствует i-й строке матрицы Уолша-Адамара и наоборот.

Тогда, очевидно, выполняется равенство

Например, для n = 2 имеем матрицу Уолша-Адамара :

,

причем

;

;

;

и матричное произведение соответствует вычислению вектора значений функции для всех .

Выражение для расчета значений коэффициентов преобразования Уолша-Адамара запишем, соответственно, в виде

.

Максимальное значение коэффициентов преобразования Уолша-Адамара булевой функции f(x) соответствует максимальному коэффициенту корреляции (похожести) последовательности этой функции и последовательностей всех аффинных функций из множества :

Последовательности аффинных функций с в (5) соответствуют инверсии (умножению на «-1») последовательностей функций из , следовательно, максимум модуля коэффициентов преобразования Уолша-Адамара булевой функции f(x) будет соответствовать максимальному коэффициенту корреляции последовательности этой функции и последовательностей всех аффинных функций из множества .

По определению нелинейности из (4) имеем:

Поскольку

справедливо равенство

откуда имеем

.

Автокорреляционная функция, обозначаемая , вычисляется по формуле [6]:

,

где и . Автокорреляционная функция является вектором, содержащим 2^n действительных значений в диапазоне .

Автокорреляция AC функции f является максимальным абсолютным значением автокорреляционной функции [6]:

.

Таким образом, математический аппарат булевых функций является удобным инструментом для описания регулярных нелинейных узлов замен, а использование преобразования Уолша-Адамара дает адекватный механизм оценки основных криптографических показателей стойкости, в частности, нелинейности компонентных булевых функций.

В то же время, использование рассмотренного математического аппарата для синтеза регулярных узлов замен через итеративное формирование компонентных булевых функций является непрактичным уже при n = 6 и вычислительно недостижимым для n > 6 [2, 3]. Перспективным направлением в этом смысле является использование недвоичных криптографических функций, описывающих отображение n-битных блоков входных данных в m-битные выходные блоки в нелинейном узле замен в виде функций отображения .

Предлагаемый подход к описанию нелинейных узлов замен через недвоичные функции отображения

Введем основные понятия и определения предлагаемого математического аппарата для описания нелинейных узлов замен через недвоичные функции и оценки их криптографических свойств.

Недвоичной (над полем) функцией от n_2 переменных является функция, осуществляющая отображение из поля всех векторов длины с элементами из в поле . Как и рассмотренные выше булевы функции, каждая недвоичная функция может быть представлена в АНФ, т.е. как сумма произведений составляющих координат:

(7)

где - уникальные константы из , суммирование и умножение также производится в поле .

Поле состоит из векторов , :

, , …, , , , , …, ,

где – векторное пространство над .

Поле изоморфно полю , , т.е. имеем взаимно-однозначное функциональное соответствие множества векторов с элементами из и двоичных векторов .

Таблицей истинности недвоичной (над полем) функции F называется последовательность с элементами из , определенная как:

Последовательностью недвоичной (над полем) функции F называется последовательность из (1,-1)-кортежей длины каждый, определенная как:

где под понимается - й бит числа .

Например, пусть , и недвоичная (над) функция задана в АНФ следующим образом:

,

где коэффициенты многочлена принадлежат полю :

, , ,.

Входными элементами такой функции являются однокоординатные вектора (скаляры) с элементами из : , , , , .

Таблицей истинности функции является последовательность с элементами из :

Последовательностью функции является последовательность из (1,-1)-кортежей длины каждый:

Рассмотрим криптографические свойства функций , реализующих отображения из в , где . Пусть есть множество таких функций , а есть множество недвоичных функций от переменных, то есть функций, реализующих отображения из в . Тогда любую функцию из можно рассматривать как состоящую из недвоичных функций от переменных, т.е. m-выходных координатных функции из . В более общем представлении, компонентная функция из является ненулевой линейной комбинацией ее координатных недвоичных функций из .

Таким образом, функцию отображения , реализующую нелинейный узел замен, запишем через множество

,

где .

В данной работе ограничимся рассмотрением функций с , т.е. будем рассматривать только функции , реализующие отображения из в .

Введенная формализация функционального отображения является естественным обобщением рассмотренного выше подхода к представлению регулярных узлов замен в виде совокупности компонентных булевых функций. Действительно, используя традиционный подход к описанию функционального отображения n-битных блоков входных данных в m-битные выходные блоки функцию , где , можно представить в виде кортежа

из булевых функций от булевых переменных каждая.

Для недвоичной функции из предыдущего примера имеем следующее соответствие:

,

где знак тождества означает тождественность правила отображения n=2-битных блоков входных данных в m=2-битные выходные блоки.

Алгебраическая степень , обозначаемая , определяется как максимальная степень многочлена представленного в АНФ.

Важные свойства булевых функций изучается с использованием преобразования Уолша-Адамара.

По аналогии с преобразованием Уолша-Адамара введем спектральное преобразование недвоичных функций следующим образом.

Спектральным преобразованием недвоичной функции есть вещественная функция :

, (8)

где под - понимается -я недвоичная аффинная функция от переменных из множества :

. (9)

Также как и вектор в случае булевого описания определяет вид линейных двоичных функций , в случае недвоичного описания вектор задает вид недвоичных аффинных функций .

Если в (8) пробегает все недвоичные линейные функции (с в (9)) будем говорить, что функция определяет *неполный спектр* недвоичной функции (спектр по линейным функциям).

Если в (8) пробегает все недвоичные линейные и аффинные функции (с в (9)) будем говорить, что функция задает *полный спектр* недвоичной функции (спектр по всем аффинным функциям).

В матричном виде введенное спектральное преобразование задается в виде матричного умножения последовательности недвоичной функции , на матрицу порядка , строки которой образованны последовательностями недвоичных линейных (для неполного спектра) и аффинных (для полного спектра) функций (аналог матрицы Уолша-Адамара порядка):

Элементами матрицы являются (1,-1)-кортежи длины каждый, определенные правилом формирования последовательности недвоичной функции.

Для рассмотренного выше примера недвоичной функции неполный спектр в матричном виде определяется следующим образом:

Полученный результат говорит о полной коррелированности последовательностей двоичных функций, в эквивалентной записи недвоичного описания, с одной или несколькими двоичными функциями.

Корреляционным преобразованием недвоичной функции есть вещественная функция :

.

Выводы

Традиционный подход к описанию и оцениванию нелинейных узлов замен состоит в представлении функции S-блока с помощью ее координатных функций, которые задаются в терминах булевой алгебры. Основными криптографическими показателями нелинейных узлов замен в терминах булевой алгебры являются регулярность (сбалансированность компонентных булевых функций), алгебраическая степень, нелинейность и автокорреляция.

Математическая модель представления S-блоков через недвоичные функции является новым направлением исследований в области формирования нелинейных узлов замен. В нашей работе были введены основные понятия и определения математического аппарата для описания нелинейных узлов с использованием одной недвоичной функции. Были разработаны и обоснованы спектральные и корреляционные преобразования криптографических недвоичных функций.

Перспективными направлениями дальнейших исследований являются разработка критериев отбора вычислительных методов синтеза нелинейных узлов замен с использованием предложенной математической модели криптографических недвоичных функций, проведение экспериментальных исследований эффективности вычислительных методов с новыми критериями, развитие математического аппарата криптографических недвоичных функций для описания S-блоков через их совокупность.

Список литературы

1. *Сорока Л.С., Кузнецов А.А., Московченко И.В., Исаев С.А. Вероятностная модель формирования нелинейных узлов замен для симметричных криптографических средств защиты информации // Системи обробки інформації. – Х.:ХУВС, 2009. - № 3 (77). – С. 101-104.*
2. *O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology,1994. – P. 133-151.*
3. *Сорока Л.С., Кузнецов А.А., Исаев С.А. Исследование вероятностных методов формирования нелинейных узлов замен // Системи обробки інформації, 2011. - № 8 (98). – С. 113 – 122.*
4. *Булева функция [Електронний ресурс] // Режим доступу: http://ru.wikipedia.org/wiki/Булева_функция.*
5. *Dawson E., Millan W., Simpson L. Designing Boolean functions for cryptographic applications // Contributions to General Algebra. - Verlag Johannes Heyn, Klagenfurt, 2000. – 12. – P. 1-22.*
6. *Clark J.A., Jacob J.L., Stepney S., Maitra S., Milan W. Evolving Boolean functions satisfying multiple criteria // Lecture Notes in Computer Science (2551).- Springer , Berlin, 2002. - 2251. - P. 246-259.*
7. *Parker M.G. Generalised S-Box Nonlinearity // NES/DOC/UIB/WP5/020/A. – 2003.*

Рецензент: .

Автор: *КУЗНЕЦОВ Александр Александрович*
Харьковский национальный университет им. В.Н. Каразина, Харьков, доктор технических наук, профессор, профессор кафедры безопасности информационных систем и технологий.
Раб. тел. - 057-752-64-15, E-Mail – kuznetsov_alex@rambler.ru.

Автор: *ИСАЕВ Сергей Александрович*
Харьковский национальный университет им. В.Н. Каразина, Харьков, аспирант кафедры безопасности информационных систем и технологий.
E-Mail – isaev.s23@gmail.com.

Автор: *ФРОЛОВ Владислав Владимирович*
Харьковский национальный университет радиоэлектроники, Харьков, магистрант кафедры безопасности информационных технологий.
E-Mail – frolvlad@gmail.com.

УДК
Кузнєцов О.О., Ісаєв С.О., Фролов В.В. Математична модель регулярних нелінійних вузлів замін з використанням недвійкових криптографічних функцій // Системи обробки інформації. – 2005. – Вип. 00 (00). – С. 00 – 00. – Рос.
Розглядається традиційна математична модель регулярних нелінійних вузлів замін з використанням сукупності мулевих функцій. Розробляється математична модель регулярних нелінійних вузлів замін з використанням недвійкових криптографічних функцій. Вводяться спектральні та кореляційні перетворення недвійкових функцій.
Табл. 0. Іл. 0. Бібліогр. 7 назв.

Кузнецов А.А., Исаев С.А., Фролов В.В. Математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций // Системы обработки информации. - 2005. - Вып. 00 (00). - С. 00- 00 . - Рус.
Рассматривается традиционная математическая модель регулярных нелинейных узлов замен с использованием совокупности булевых функций. Разрабатывается математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций. Вводятся спектральные и корреляционные преобразования недвоичных функций.

Kuznetsov A.A., Isaev S.A., Frolov V.V. Mathematical model of regular nonlinear substitution components with the use of non-binary cryptographic functions // Sistemi obrobki informacii. - 2005. - Issue 00 (00). - P. 00- 00 . - Rus.
Traditional mathematical model of regular nonlinear substitution components using a set of Boolean functions is considered. Mathematical model of regular nonlinear substitution components with non-binary cryptographic functions is developed. Spectral and correlation transforms of non-binary functions are introduced.