УДК 638.322

А.Д. Плотников[1], Е.В. Васильев[1]

[1]кафедра «Безопасность информационных систем» Восточноукраинского национального университета имени В.Даля

ПРИМЕНЕНИЕ БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ВСКРЫТИЯ ЗНАЧЕНИЙ КЛЮЧА В КРИПТОСИСТЕМЕ

В работе рассматриваются некоторые методы вскрытия значений ключа криптосистемы, используя описание итераций шифрования системой булевых функций. Приводится описание поставленного эксперимента и полученные в результате данные.
Ключевые слова: булевы функции, криптосистемы, шифрование, ключ шифрования.

Введение

Как известно, всякая криптосистема производит шифрование открытого текста M, представляющего булев вектор длины n в зашифрованный текст C — булев вектор той же длины, с помощью ключа K, также представляющего собой булев вектор длины s [1].

Многие криптосистемы шифрование открытого текста производят в несколько раундов (итераций). Преобразование входной информации на каждом раунде можно представить как черный ящик, на вход которого поступает текст (исходный или преобразованный на предыдущих раундах) в виде булева (двоичного) вектора M_1, булев вектор K*, сформированный из исходного ключа [3]. Выход представляет собой булев вектор M_2 — преобразованная входная информация (Рис. 1).

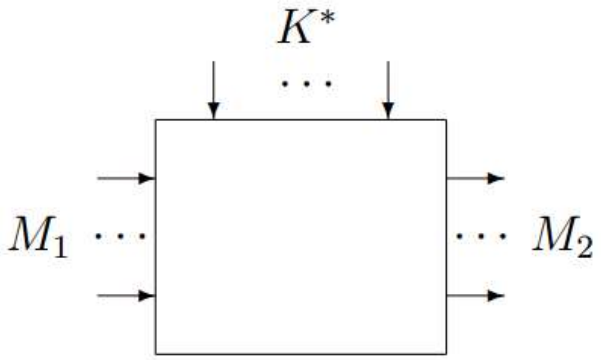

Рис. 1

Таким образом, каждый раунд шифрования можно рассматривать как преобразование, осуществляемое булевым многополюсником. Цель данной работы состоит в том, что используя представление раунда шифрования в виде черного ящика, выполнить компьютерный эксперимент по нахождению значению ключа исследуемой криптосистемы.

Ясно, что мы ориентируемся на взлом симметричной криптосистемы типа DES и AES.

Идеология эксперимента

Пусть $M_1 = \{m_1^1, m_1^1, \ldots, m_n^1\}$, $M_2 = \{m_1^2, m_1^2, \ldots, m_n^2\}$, и $K^* = \{k_1^*, k_1^*, \ldots, k_s^*\}$. Тогда процедуру шифрования на каждом раунде можно описать системой из n булевых функций:

$$\begin{cases} m_1^2 = f_1(M_1, K^*) \\ m_2^2 = f_2(M_1, K^*) \\ \ldots \\ m_n^2 = f_n(M_1, K^*) \end{cases} \quad (1)$$

Выгоднее всего булеву функцию представить строкой истинности, т.к. это наиболее экономный способ [3]. Булевы функции системы (1), представленные в виде векторов истинности построить не трудно.

Мы будем полагать, что нам известны значения функций m_i^2 (i = 1, 2, ...,n). Т.е. либо это последний раунд шифрования, либо значение вектора M_2 найдено ранее.

Для хранения вектора истинности требуется 2^{n+m} ячеек памяти. Согласно системе (1) имеется n таких функций. Если функция равна 1 или 0, то это значение определяет компоненты вектора истинности, равные соответственно 1 или 0, которые следует выбирать. Такие компоненты назовём выбранными для каждой функции.

Напомним, что каждая компонента вектора истинности определяет определенный набор значений переменных, от которых зависит эта функция. Ясно, что для всех функций системы (1) существует единый набор значений переменных, на которых функции системы принимают известные значения. Чтобы определить такой набор, необходимо выполнить покомпонентную конъюнкцию выбранных компонент.

Представляет интерес определить, как велико может быть подмножество наборов, удовлетворяющих системе (1).

Проведение эксперимента

Для проведения эксперимента была написана программа, которая генерирует случайные векторы истинности булевых функций. Интерфейс программы представлен на Рис. 2. Все функции являются псевдо бент-функциями, т.е. имеют одинаковое количество нулей и единиц в векторе истинности каждой булевой функции. В будущем предполагается проведение эксперимента с реальными булевыми функциями на примере действующих криптосистем (например, DES).

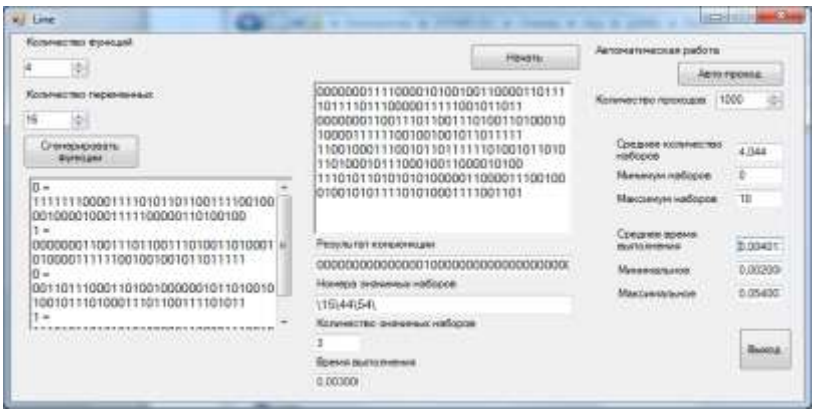

Рис. 2. Программный интерфейс

Программа позволяет устанавливать размерность системы булевых функций с помощью двух параметров: количество генерируемых функций (векторов истинности) и количество переменных в них. Каждая булева функция, представленная вектором истинности, может быть равна нулю или единице. Перед началом работы выполняются следующие подготовительные операции. Если функция равна единице, то ее вектор остаётся без изменений, если же нулю, то ее вектор истинности инвертируется. В итоге получаем некую систему булевых функций, представленных в виде векторов истинности, каждая из которых равна 1.

Как уже было сказано выше, для определения наборов переменных, удовлетворяющих системе (1), необходимо выполнить покомпонентную конъюнкцию выбранных компонент. После проведения данной операции получаем результирующий вектор истинности. Искомые наборы в нём представлены единицами. Также программа выводит номера этих наборов и их количество, т.к. производить такой анализ вручную может быть очень неудобно из-за большого объёма данных.

Для получения необходимых экспериментальных данных программа способна работать в автоматическом режиме, проводя эксперимент необходимое количество раз. Для каждого прохода генерируется новый набор векторов истинности. В итоге мы получаем данные о среднем количестве наборов, удовлетворяющих системе (1), для заданных размеров системы булевых функций, сколько их было минимум и максимум, а также сведения о времени выполнения.

Для проведения эксперимента было выбрано значение в 1000 проходов программы. Количество переменных от 4 – до 1024 (все значения являются степенями числа 2), количество функций от 4 – до 10.

Больше всего нас будет интересовать среднее количество наборов, удовлетворяющих системе, при заданной размерности. После проведения эксперимента имеем следующие результаты, представленные в таблице:

Таблица 1.

Результаты эксперимента

ер\фун	4	5	6	7	8	9	10
4	0,959	0,466	0,212	0,154	0,061	0,028	0,019
8	1,893	1,009	0,446	0,272	0,089	0,079	0,032
16	3,868	1,908	0,901	0,464	0,265	0,11	0,055
32	7,908	3,874	1,997	1	0,486	0,224	0,118
64	15,769	7,789	3,894	1,918	0,928	0,468	0,215
128	31,695	15,7	8,034	3,901	1,951	1,04	0,496
256	64,154	31,624	15,599	7,971	3,954	1,972	0,945
512	128,03	64,921	32,019	16,029	8,045	4,049	2,004
1024	256,45	127,38	64,317	32,205	15,888	8,054	4,059

Столбцы представляют количество функций в системе, строки – количество переменных, от которых зависят булевы функции системы. На пересечении строки и столбца находится значение, представляющее среднее количество значимых наборов для заданной размерности системы булевых функций на 1000 проходов.

Несложно заметить закономерность: количество наборов значений переменных, которые удовлетворяют заданной системе, остаётся примерно одинаковым, если при увеличении количества функций на 1, количество переменных в системе удваивается. Незначительными отклонениями можно пренебречь, как погрешностями.

Следующая диаграмма наглядно демонстрирует данную закономерность.

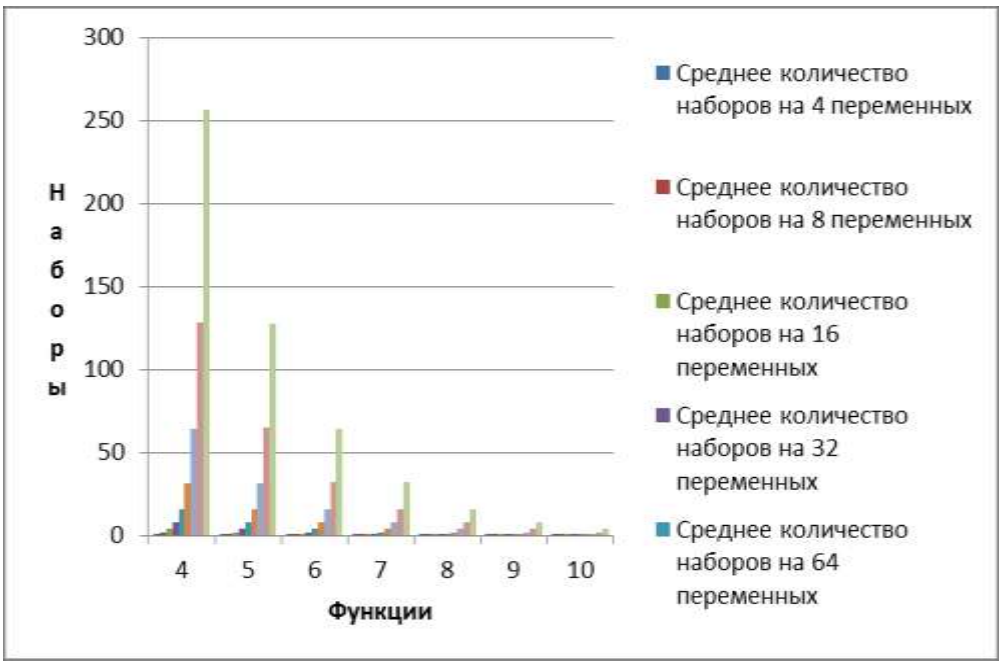

Рис. 3. Диаграмма полученных данных

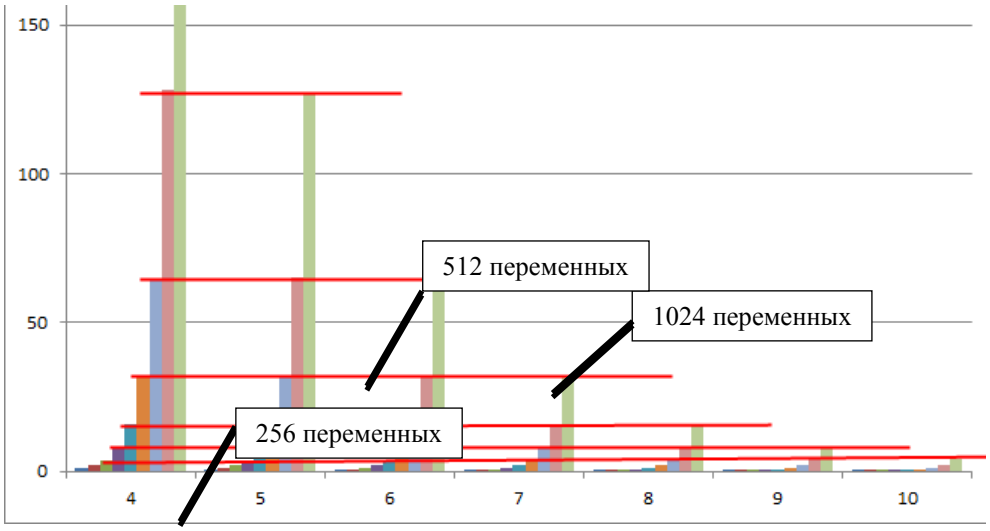

Рис. 4. Детализированные данные диаграммы

На диаграмме (Рис. 4) ось абсцисс указывает количество булевых функций в системе, а ось ординат – среднее количество наборов, удовлетворяющих заданной системе для различного числа переменных, от которых зависят функции системы. Таким образом, для фиксированного количества функций в системе, построен столбик, указывающий количество удовлетворяющих систему наборов. На рис.4 горизонтальные линии отображают равенство значений при разных размерностях системы. К примеру, имеем одинаковое среднее количество наборов на 4, 5 и 6 функциях при 256, 512 и 1024 переменных соответственно.

Также из таблицы можно установить, что количество значимых наборов равно:

1/4 количества переменных на 4 функциях;
1/8 количества переменных на 5 функциях;
1/16 количества переменных на 6 функциях;
и т.д.

В соответствии с этим можно получить формулу для подсчёта среднего количества наборов, удовлетворяющих системе (1):

$$N(f) = \frac{1}{2^{f-2}} * p \quad , \tag{2}$$

где f – количество функций, p – количество переменных.

Формула справедлива для данных, полученных в проведённом эксперименте. Однако здесь использовались псевдослучайные системы булевых функций, и достоверно неизвестно какие данные можно получить на реальных системах. Поэтому необходимо дальнейшее исследование и проведение эксперимента на булевых функциях, полученных для существующих криптосистем, например для DES.

Выводы

В результате проведения эксперимента были установлены следующие данные. При покомпонентной конъюнкции компонент в системе булевых функций, представленных псевдослучайными векторами истинности, обнаружены две закономерности. Количество значимых наборов остаётся примерно одинаковым, если при увеличении количества функций на одну, количество переменных удваивается. И среднее количество наборов, конъюнкция которых равна единице, можно вычислить по формуле (2).

Данные эксперимента являются предварительными и требуют дальнейшего исследования.

Литература

1. Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии – М.: МЦНМО, 2004 – 470 с.
2. Агафонова И.В. Криптографические свойства булевых функций. Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD», 2007. — 24 с. (http: //www.dha.spb.ru/)
3. Плотников А.Д., Петров А.С. Некоторые особенности анализа симметричных криптосистем. Інформаційна безпека, №1 (3), 2010

Надійшла до редколегії 19.03.2013 р.

Рецензент: д.т.н., проф. Петров А.С.

А.Д. Плотніков, Є.В. Васільев

ЗАСТОСУВАННЯ БУЛЕВИХ ФУНКЦІЙ ДЛЯ РОЗКРИТТЯ ЗНАЧЕНЬ КЛЮЧА У КРИПТОСИСТЕМЕ

В роботі розглядаються деякі методи викриття значень ключа криптосистеми, використовуючи опис ітерацій шифрування системою булевих функцій. Приводиться опис поставленого експерименту та отримані в результаті дані.

Ключові слова: булеві функції, криптосистеми, шифрування, ключ шифрування.

A.D.Plotnikov, E.V.Vasilyev

APPLICATION OF BOOLEAN FUNCTIONS FOR OPENING KEY VALUES IN THE CRYPTOSYSTEM

This paper discusses some methods of uncovering of the key values of the cryptosystem using the description of iterations encryption system of Boolean functions. Presented the description of the experiment and the gathered resulting data.

Keywords: boolean functions, cryptosystems, encryption, encryption key.