УДК 004.032.26

ИССЛЕДОВАНИЕ ВРЕМЕННЫХ ХАРАКТЕРИСТИК И УСТОЙЧИВОСТИ ШИФРА К КРИПТОАНАЛИЗУ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ОПЕРАЦИОННЫХ БЛОКОВ

© 2012 О. И. Лапшиков[1], В. Н. Лопин[2]

[1]аспирант каф. программного обеспечения и администрирования информационных систем факультета ИВТ
e-mail: woodlin@mail.ru
[2]докт. техн. наук,
профессор каф. программного обеспечения и администрирования информационных систем,
e-mail: kzis3@yandex.ru

Курский государственный университет

В работе рассматривается алгоритм блочного шифрования с использованием нейросетевых управляемых логических модулей, реализующих взаимно-обратные управляемые перестановки, его временные характеристики, в также стойкость этого алгоритма к дифференциальному и линейному криптоанализу.

Ключевые слова: нейросетевые логические модули, блочный шифр, управляемые перестановки, скорость шифрования, криптоанализ.

Настоящая работа является продолжением исследований по использованию иерархических нейроструктур в задачах блочного шифрования [Лопин, Лапшиков 2012; Лопин, Захаров 2004] и посвящена анализу временных характеристик и устойчивости шифра к дифференциальному и линейному криптоанализу. Необходимо отметить, что в работе под устойчивостью к дифференциальному и линейному криптоанализу понимается некоторое N – количество пар открытых текстов и шифртекстов, необходимых криптоаналитику для раскрытия шифра.

При проведении исследования рассматривается вариант блочного шифрования, схема которого представлена на рисунке 1. Приведенная схема шифрования оперирует с 16-битовыми входными и выходными блоками. Входной блок данных обрабатывается с помощью повторения двух раундов, включающих замены и перестановки битов, а также сложения с раундовым ключом шифрования. Используемые в алгоритме операции перестановки битов осуществляются при помощи нейросетевых операционных блоков [Лопин, Лапшиков 2012].

Исходный n-битовый блок данных, длина которого равна степени числа 2, разделяется на два подблока: $A = a_1..a_{n/2}$ и $B = b_1..b_{n/2}$. Каждый подблок является входом нейросетевых операционных блоков *NET*1 и *NET*2, которые осуществляют перемешивание и замену в выходных блоках. Следует отметить, что перестановки битов, выполненные блоками *NET*1 и *NET*2, являются взаимно обратными. Каждый нейросетевой блок, является комбинацией настраиваемых иерархических нейронных сетей. Работа блоков, а следовательно, и итоговая таблица битовых перестановок зависит непосредственно от множества векторов настройки $R1$ и $R2$ блоков *NET*1 и *NET*2 соответственно и шифруемых подблоков A и B. При оценке устойчивости шифра к криптоанализу рассматривается случай, при котором $R = const$ на всех раундах шифрования. Работу такого блока можно представить в виде замены элементов вектора

$A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ на соответствующие элементы вектора $A' = (a'_0, a'_1, a'_2, a'_3, a'_4, a'_5, a'_6, a'_7)$.

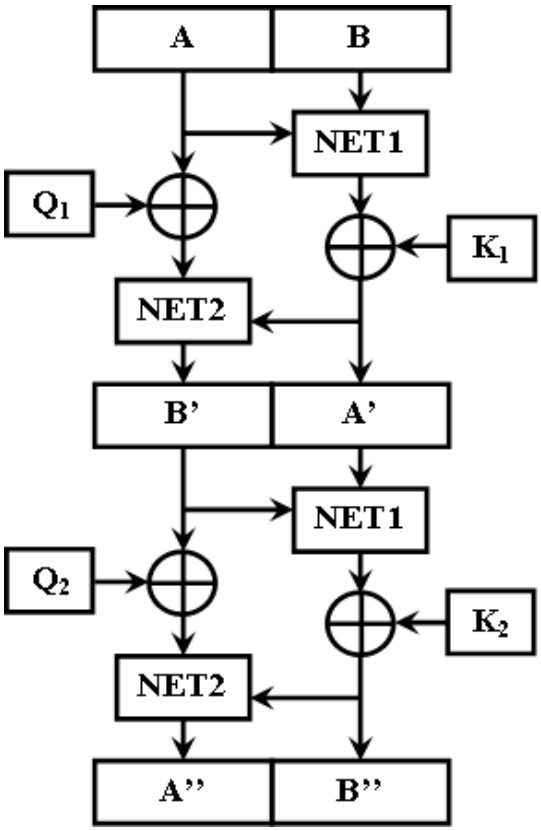

Рис 1. Алгоритм шифрования

Для выполнения операции сложения с ключом используется побитовое сложение по модулю 2 (XOR) между битами раундовых ключей K и Q с битами подблоков данных, поступающих на вход раунда. Обычно [Молдовян, Молдовян, Еремеев 2004] в алгоритме шифрования раундовые ключи извлекаются из какого-либо основного ключа. Однако в данном алгоритме рассмотрен общий случай, при котором в каждом раунде используются ключи Q_1, Q_2, K_1, и K_2, полученные некоторым случайным образом.

При расшифровании необходимо использовать последовательность действий алгоритма шифрования в том же порядке, то есть используются раундовые ключи $Q'_1 = K_2$, $Q'_2 = K_1$, $K'_1 = Q_2$, и $K'_2 = Q_1$.

Таким образом, алгоритмы шифрования и расшифрования имеет идентичные структуры.

В данной работе проанализирован описанный выше алгоритм шифрования на устойчивость к дифференциальному и линейному криптоанализу.

Исследование устойчивости шифра к дифференциальному и линейному криптоанализу можно выполнить следующим образом. Рассматривается элементарная система блочного шифрования, состоящая из двух нейросетевых операционных блоков [Лопин 2012], реализующая вышеприведенный алгоритм шифрования, представленный на рисунке 1.

При анализе рассматривается ситуация наиболее благоприятная для криптоаналитика. Под наиболее благоприятной понимается ситуация при которой:

– аналитик имеет в распоряжении неограниченное количество пар открытых текстов и шифртекстов для анализа;

– при шифровании используется одна прямая и соответствующая ей обратная перестановка ($R = const$ для всех раундов шифрования);

– система в процессе выполнения прямой и обратной перестановок возвращает элементы выходного потока в той же последовательности, что и во входном. Данный вариант работы шифратора можно записать как замену элементов вектора $A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ на соответствующие элементы вектора $A' = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$.

Выбор пар анализируемых текстов осуществлялся на основании следующих принципов. Количество анализируемых разностей должно быть достаточно для нахождения всех битов используемого секретного ключа. При этом каждая из анализируемых разностей должна при своем прохождении через раунды шифрования затрагивать как можно меньше блоков замены (большое количество затрагиваемых блоков возможно лишь в том случае, когда вероятность прохождения через блок равна 1) и иметь как можно большую вероятность получения выходной разности. Для нахождения битов, используемых ключей при помощи дифференциального криптоанализа с учетом описанных выше требований и принятых условий шифрования на вход шифратора может быть подана любая последовательность бит, например $A = 00000000$ и $B = 00000000$.

Схема преобразования битового потока в системе шифрования представлена на рисунке 2. Из данной схемы видно, что исходя из принятых условий и ограничений потоки, поданные для обработки на $NET1$ и $NET2$, остаются в первоначальном виде. Отсюда процесс нахождения шифротекста можно представить в виде последовательности действий:

$$A' = NET1(B) \oplus K1 = B \oplus K1;\ B' = NET2(A \oplus Q1) = A \oplus Q1.$$

$$A'' = NET1(B') \oplus K2 = B' \oplus K1;\ B'' = NET2(A' \oplus Q2) = A' \oplus Q1.$$

При этом шифротекст можно определить по формуле

$$A'' = A \oplus Q1 \oplus K2;\ B'' = B \oplus K \oplus Q2. \qquad (1)$$

Поскольку криптоаналитику известны начальные и конечные последовательности A, B, A'', B'', можно сделать вывод о том, что для гарантированного нахождения ключей шифрования ему необходимо проанализировать все варианты ключей шифрования, при которых A отображается в A'' и B – в B'' соответственно. Все возможные варианты ключей для анализа можно получить прямым перебором ключей $K1$ и $Q1$, при этом ключи:

$$K2 = A'' \oplus A \oplus Q1;\quad Q2 = A'' \oplus A \oplus K1.$$

С учетом того, что ключи $K1$ и $Q1$ являются n-битовыми последовательностями, можно утверждать, что для вскрытия шифра методом дифференциального криптоанализа аналитику необходимо перебрать $2^{n/2}$ исходных текстов.

Для оценки устойчивости шифра к линейному криптоанализу используются аналогичные дифференциальному криптоанализу благоприятные условия для криптоанализа. В процессе рассматриваемого криптоанализа аналитик должен построить линейные статистические аналоги и попытаться найти биты ключа. Очевидно, что для

нахождения наиболее эффективных аналогов необходимо перебрать все возможные комбинации, в результате которых возможно получить эффективные аналоги.

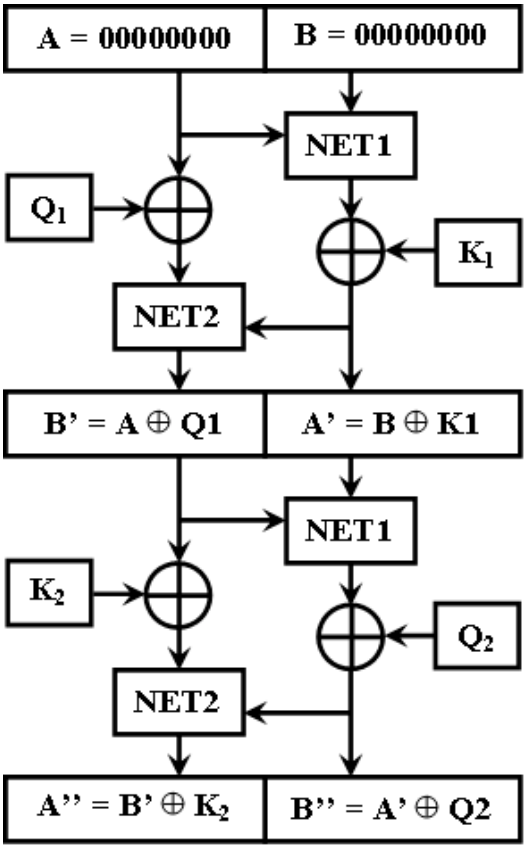

Рис 2. Шифрование потоков

Для рассматриваемого варианта алгоритма шифрования (1) можно сделать утверждение о том, что любой i-й бит шифротекста является статистическим аналогом исходного текста. Это можно представить следующей зависимостью:

$$a_i \oplus S = a_i'';\ b_i \oplus S1 = b_i'',$$

где $S = Q1 \oplus K2$; $S1 = K1 \oplus Q2$.

Поскольку аналитику известны значения битов исходного и шифротекста, то ему, как и в случае с дифференциальным криптоанализом, необходимо найти ключи $K1$ и $Q1$ полным перебором.

В таблице 1 приведено количество текстов, необходимых для взлома шифра методами дифференциального и линейного криптоанализа.

Таблица 1

Количество необходимых для криптоанализа текстов

Количество бит в блоке	***N***	***Ln*(*N*)**
8	16	2,772589
16	256	5,545177
32	65536	11,09035
64	4,29*E*+09	22,18071
128	1,84*E*+19	44,36142

В качестве примера приводится анализ времени, необходимого для шифрования 101 kb информации программой, реализующей рассматриваемый алгоритма шифрования. Данные, полученные в ходе практического эксперимента, приведены в таблице 2.

Таблица 2

Время шифрования данных

Количество бит в блоке	**Время шифрования, мс**
8	20063
16	26985
32	36188
64	47984
128	69157

На рисунках 3 и 4 представлены графики зависимостей времени шифрования и устойчивости шифра к криптоанализу от размера блока данных.

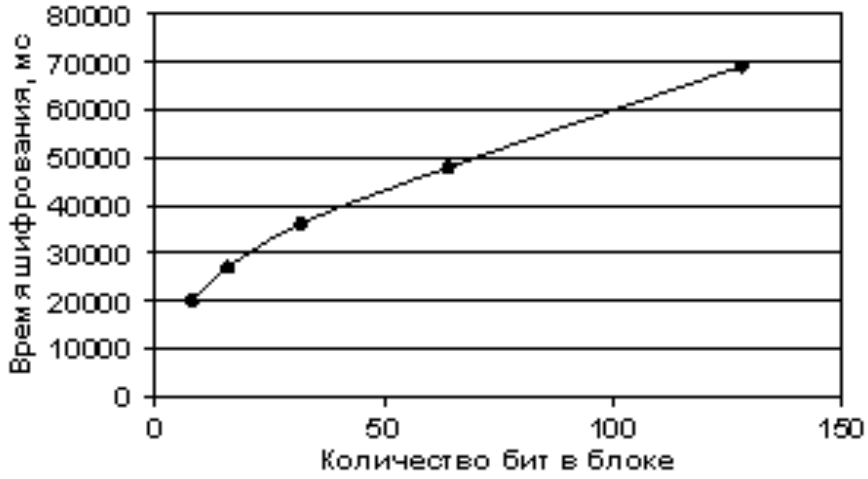

Рис 3. Зависимость времени шифрования от размера блока данных

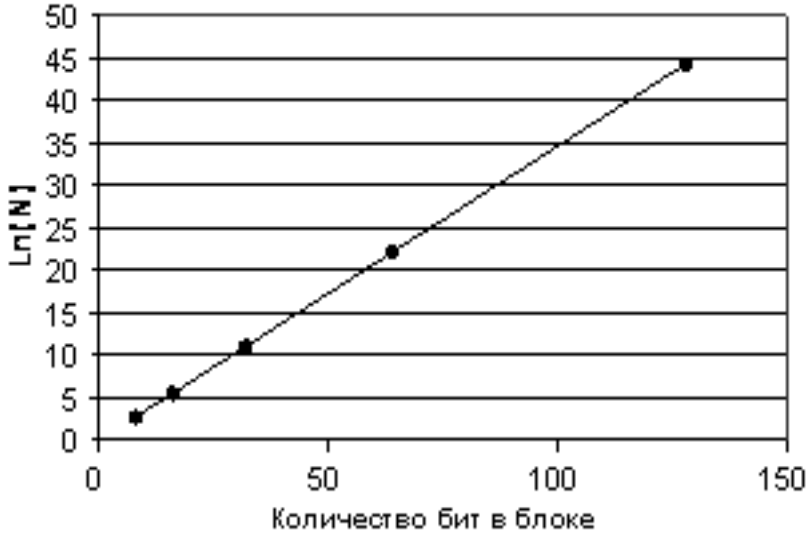

Рис 4. Зависимость устойчивости шифра к криптоанализу от размера блока данных

Из результатов проведенной оценки устойчивости рассматриваемого алгоритма шифрования к дифференциальному и линейному криптоанализу, а также практического эксперимента по оценке времени шифрования фиксированного объема данных можно сделать следующие выводы:

1) устойчивость рассматриваемого алгоритма к дифференциальному и линейному криптоанализу зависит от длины шифруемого блока;

2) с увеличением длины шифруемого блока устойчивость к дифференциальному и линейному криптоанализу растет экспоненциально;

3) время, необходимое для осуществления шифрования по рассматриваемому алгоритму, пропорционально размеру шифруемых блоков данных.

Библиографический список

Лопин В. Н., Лапшиков О. И. Блочное шифрование на основе нейросетевых операционных блоков, реализующих взаимно-обратные управляемые перестановки // Информация и безопасность: регион. науч.-техн. журнал, Воронеж, 2012. №1. С. 105–108.

Лопин В. Н., Захаров И. С. Шифрование бинарного информационного потока методом периодических перестановок на основе нейросетевых логических модулей // Телекоммуникации. М.: Наука и технологии, 2004. №12. С. 31–35.

Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.