Удальцов Валерий Анатольевич
аспирант
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
г. Санкт-Петербург

DOI 10.21661/r-471085

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СОКРАЩЕНИЯ КОЛИЧЕСТВА РАУНДОВ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА УСТОЙЧИВОСТЬ К СТАТИСТИЧЕСКИМ АТАКАМ И ПРОИЗВОДИТЕЛЬНОСТЬ АЛГОРИТМА ШИФРОВАНИЯ «КУЗНЕЧИК»

Аннотация*: целью данной статьи является определение возможности модификации алгоритма шифрования «Кузнечик» путем сокращения раундов криптографических преобразований для увеличения скорости работы, при сохранении его стойкости к статистическим атакам. В работе описываются результаты исследований влияния сокращения количества раундов криптографических преобразований на устойчивость к статистическим атакам и производительность данного алгоритма шифрования, в рамках которого с помощью метода статистического теста «Стопка книг» проведен анализ 100 последовательностей размером 2^{28} каждая. В результате исследования было выявлено, что при использовании хотя бы 3 раундов преобразований генерируемая последовательность неотличима от случайной.*

Ключевые слова*: криптография, сокращение раундов, ускорение шифрования, блочный алгоритм шифрования, статистический криптоанализ, «Кузнечик», стопка книг.*

Введение

Одним из основных показателей надежности алгоритма шифрования является неотличимость генерируемого шифртекста от случайной последовательности, за счет чего обеспечивается устойчивость к статистическому криптоанализу.

Однако это требует вовлечение значительных ресурсов, сокращение которых возможно за счет применения легковесной криптографии.

Одной из наиболее полных и обобщающих работ по легковесной криптографии является вышедшая в двух частях статья [3–4], в рамках которой определяются два основных направления развития, нацеленных на уменьшение объемов затрачиваемых ресурсов при проведении криптографических вычислений, а именно: разработка ориентированных на аппаратную реализацию алгоритмов и оптимальная реализация уже разработанных алгоритмов. В свою очередь, оптимальную реализацию алгоритмов также можно разделить на два направления: оптимизация под конкретную платформу, данной тематике посвящены предыдущие работы [9–10], и модификация алгоритмов. Одним из наиболее простых способов модификации блочных алгоритмов является сокращение количества раундов криптографических преобразований, что гарантировано ведет к увеличению скорости шифрования, но также приводит к ухудшению стойкости шифра, а, следовательно, требует проведения криптоанализа для определения допустимого количества раундов. Данной тематике посвящена работа, рассматривающие наиболее распространенный блочные алгоритм AES [1]. С целью определения возможности применения данного способа к отечественному блочному алгоритму шифрования «Кузнечик», представленному в ГОСТ 34.12, в рамках этой работы были проведены исследования влияния сокращения количество раундов криптографических преобразований на статистические характеристики данного шифра.

Описание алгоритма «*Кузнечик*»

Алгоритм шифрования «Кузнечик» разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО «ИнфоТеКС». Он описан в ГОСТ Р 34.12–2015 «Информационные технологии. Криптографическая защита информации. Режимы работы блочных шрифтов», как базовый блочный шифр с длиной блока 128 бит и длиной ключа 256 бит, и предназначен для применения в криптографических методах обработки и защиты информации, в том числе для обеспечения конфиденциальности, аутентичности и целостности

информации при ее передаче, обработке и хранении в автоматизированных системах.

Данный алгоритм имеет LSX структуру, включающую в себя следующие преобразования:

– преобразование X, в рамках которого выполняется операция сложение по модулю два над двумя двоичными строками равной длины и обеспечивается смешение с раундовым кличем;

– преобразование S – осуществляет нелинейное биективное преобразование, в качестве которого используется подстановка, значения для которой приведены в пункте 4.1.1 рассматриваемого стандарта, а в качестве индекса используется значения блока входных данных;

– преобразование L осуществляет шестнадцать раундов преобразования R, которое выполняет линейное преобразование входного блока данных, представляющее собой сумму произведений 8-битных элементов, входной двоичной строки, с соответствующими константами, последующий сдвиг всех элементов в сторону младшего и занесение результата линейного преобразования на место старшего 8-битного элемента.

Зашифрование открытого текста осуществляется с помощью 10 раундов описанных выше криптографических преобразований, при этом последний раунд отличается от остальных и состоит из одного преобразование X. Для каждого раунда используется отдельный итерационный ключ, получаемый путем развертки секретного ключа [2].

Описание теста «*Стопка книг*»

Алгоритм «Стопка книг» в качестве статистического теста для случайных чисел был предложен в работе [8]. Исследования статистических свойств алгоритмов шифрования с помощью данного теста представлены в работах [5–7].

С помощью данного алгоритма осуществляется проверка гипотезы о том, что элементы выборки Z, сформированной путем зашифрования N блоков открытого текста, входящих в алфавит A, имеют равномерное распределение.

На момент начала тестирования алфавит A фиксируется в некотором произвольном порядке и разбивается на две непересекающиеся последовательности $A_1 = \{1,2,\ldots,K\}$ и $A_2 = \{K+1,\ldots,S\}$, при этом последовательность A_1 определяется как «верхняя часть» «стопки книг». На первом шаге определяется индекс n первого элемента последовательности Z в алфавите A, после чего данный элемент перемещается в начало алфавита и данный шаг повторяется с использованием следующего элемента выборки. При этом осуществляется подсчет количества попаданий элементов выборки Z в последовательность A_1, определенную для конкретного шага, итоговое число которых обозначено V. Обработка результатов осуществляется по формуле 1 [7]:

$$x^2 = \frac{(V-NP_1)^2}{NP_1} + \frac{((N-V)-N(1-P_1)^2)}{N(1-P_1)},\ P_1 = \frac{|A_1|}{S}, \quad (1)$$

где S – размер алфавита A; P_1 – вероятность попадания символа алфавита A в последовательность A_1. При этом если x^2 не превышает квантиль распределения хи-квадрата с одной степенью свободы, равной 6.64, то гипотеза о равномерности распределения элементов выборки принимается, иначе – отвергается.

Исследование алгоритма «Кузнечик»

Для исследования статистических характеристик алгоритма шифрования «Кузнечик» был проведен эксперимент, в рамках которого получаемый шифртекст анализировался с помощью теста «Стопка книг». При формировании тестируемой последовательности 128 бит открытого текста были представлены в виде четырех 32 битных частей, значение каждой из которых менялось от 0 до 2^{32} с шагом 2^4, три оставшиеся при этом обнулялись. Данные последовательности были сформированы для 100 случайных ключей. При проведении статистического теста шифртекста для алфавита A был выбран размер символа алфавита равный 32 бита. Размер «верхней части» «стопки книг» в соответствии с рекомендациями, приведенными в [8], был выбран в размере 2^{16}.

Исходя из рекомендаций, представленных в работе [5], реализация данного алгоритма была осуществлена с использованием связного списка, хранящего элементы «верхней части» «стопки книг» и хэш-таблицы, хранящей ссылки на элементы списка и использующей в качестве ключей значения самих элементов.

Шифрование открытого текста для формирования тестируемой последовательности осуществлялось с помощью графического процессора.

В таблице 1 представлены результаты теста проведенного эксперимента (замеры скорости производились с использованием процессора Intel i7–3537U и запуском вычислений в одном потоке).

Таблица 1

Зависимость процента экспериментов, при которых x^2 превышает квантиль распределения хи-квадрата с одной степенью свободы и скорости шифрования от количества раундов

Номер раунда	*Номер изменяемой части открытого текста*				*Скорость шифрования, Мбайт/с*
	1	*2*	*3*	*4*	
1	100	100	100	100	55.35
2	8	7	6	9	27.97
3	0	1	1	3	18.68
4	0	0	3	0	14.02
5	0	0	4	0	11.21
6	1	0	0	0	9.34
7	0	0	0	0	8.00
8	0	0	0	0	6.91
9	0	0	0	0	6.22
10	0	0	0	0	6.21

Исходя из расчетов, приведенных в [7] и полученных из модифицированной формулы 1, для случая тестирования 100 последовательностей сгенерированных с использованием случайных ключей, можно утверждать, что распределение шифртекста не равномерно, если в ходе эксперимента полученное количество x^2 превышающих квантиль распределения хи-квадрата более 7. С учетом этого можно утверждать, что уже после 3 раундов преобразований генерируемая последовательность неотличима от случайной.

Заключение

В данной работе было исследовано влияние сокращения количества раундов криптографических преобразований на статистические характеристики алгоритма шифрования «Кузнечик» с использованием статистического теста «стопка книг», в рамках которого были проанализированы 100 последовательностей

размером 2^{28} каждая. Исходя из полученных результатов, видно, что уже после 3 раундов преобразований генерируемая последовательность неотличима от случайной, при этом скорости затрачиваемая на вычисления сокращается в 8 раз.

Список литературы

1. Security of the AES with a Secret S-box / T. Tiessen, L. Knudsen, S. Kölbl, and Martin M. Lauridsen // Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8–11, 2015, Revised Selected Papers.

2. ГОСТ Р 34.12–2015. Информационные технологии. Криптографическая защита информации. Блочные шрифты. – Введ. 19.06.2015 // ТК26: Информационный портал технического комитета по стандартизации «Криптографическая защита информации». [Электронный ресурс]. – Режим доступа: http://www.tc26.ru/standard/gost/GOST_R_3412–2015.pdf

3. Жуков А.Е. Легковесная криптография. Ч. 1 // Вопросы кибербезопасности. – 2015. – №1 (9). – С. 26–43.

4. Жуков А.Е. Легковесная криптография. Ч. 2 // Вопросы кибербезопасности. – 2015. – №2 (10). – С. 2–10.

5. Лысяк А.С. Анализ эффективности градиентной статистической атаки на блоковые шифры RC6, MARS, CAST-128, IDEA, Blowfish в системах защиты информации / А.С. Лысяк, Б.Я. Рябко, А.Н. Фионов // Вестник СибГУТИ. – 2013. – №1 (21). – С. 85–109.

6. Пестунов А.И. Предварительная оценка минимального числа раундов легковесных шифров для обеспечения их удовлетворительных статистических свойств // Прикладная дискретная математика. Приложение. – 2015. – №8. – С. 66–68.

7. Пестунов А.И. Статистический анализ современных блочных шифров // Вычислительные технологии. – 2007. – Т. 12. – №2. – С. 122–129.

8. Пестунов А.И. Теоретическое исследование свойств статистического теста «стопка книг» // Вычислительные технологии. – 2006. – Т. 11. – №6. – С. 96–102.

9. Удальцов В.А. Оптимизация скорости работы блочных алгоритмов шифрования / В.А. Удальцов, В.Э. Павлов // Приоритетные направления развития

науки и образования: Сборник материалов Международной научно-практической конференции. – Чебоксары, 2017. – С. 76–80.

10. Удальцов В.А. Увеличение скорости работы алгоритма шифрования «Кузнечик» с использование технологии CUDA / В.А. Удальцов, В.Э. Павлов // Теория. Практика. Инновации. – 2017. – №4 (16). – С. 5–11.