УДК 004.056

Н. А. Капалова, Ардабек Хомпыш,
Д.С. Дюсенбаев, О.Т. Сулейменов
Институт информационных и вычислительных технологий МОН РК,
Алматы, Республика Казахстан

ИССЛЕДОВАНИЕ «ЛАВИННОГО ЭФФЕКТА» РАЗРАБОТАННОГО АЛГОРИТМА ШИФРОВАНИЯ

Аннотация. *В данной статье рассмотрена модификация ранее разработанного алгоритма блочного шифрование EM [1] с целью его адаптации к легковесным алгоритмам шифрования. Приведены результаты исследования «лавинного эффекта» для разработанного алгоритма шифрования.*

N.Al. Kapalova, Ardabek Khompysh,
D.S. Dyussenbayev, O.T. Suleimenov
Institute of Information and Computational MES RK
Almaty, Republic of Kazakhstan

RESEARCH OF DEVELOPED ALGORITHMS ON THE CRITERIA «AVALANCHE EFFECT»

Abstract. *This article discusses a modification of the previously developed block encryption algorithm EM [1] in order to adapt it to lightweight encryption algorithms. The results of the study of the "avalanche effect" for the developed encryption algorithm are presented.*

С каждым годом увеличивается количество различных интеллектуальных устройств, имеющих доступ к сети Интернет. Появились много новых областей, таких как Интернет вещей, сенсорные сети, распределенные системы управления и т.д., в которых устройства с высокими ограничениями связаны между собой, обмениваются данными друг с другом по беспроводной сети и обеспечивают совместное выполнение некоторых задач. Поскольку большинство современных криптографических алгоритмов были разработаны для настольных и серверных сред, многие из них не подходят для устройств, имеющих ограничения на используемые ресурсы памяти, вычислительную мощность, источники питания и т.д. Исследования в этом направлении ведутся в области «легковесной криптографии» (LWC – lightweight cryptography), имеющей целью

создание быстрых и надежных алгоритмов шифрования с определенными ограничениями в использовании ресурсов.

В данной статье представлены результаты разработки нового легковесного алгоритма шифрования.

Структурная схема предлагаемого легковесного алгоритма шифрования приведена на рис. 1. Основные параметры алгоритма: длина блока – 64 бита, длина ключа – 80 бит, количество раундов шифрования – 32. В алгоритме используются методы блочной перестановки: P-блок, сложение по модулю 2 (xor), нелинейные преобразования в виде S-блоков.

Перед началом шифрования входные данные разбиваются на блоки размером 64 бита. Последний блок при необходимости дополняется по оговоренным правилам (например, нулями). Далее производятся следующие преобразования.

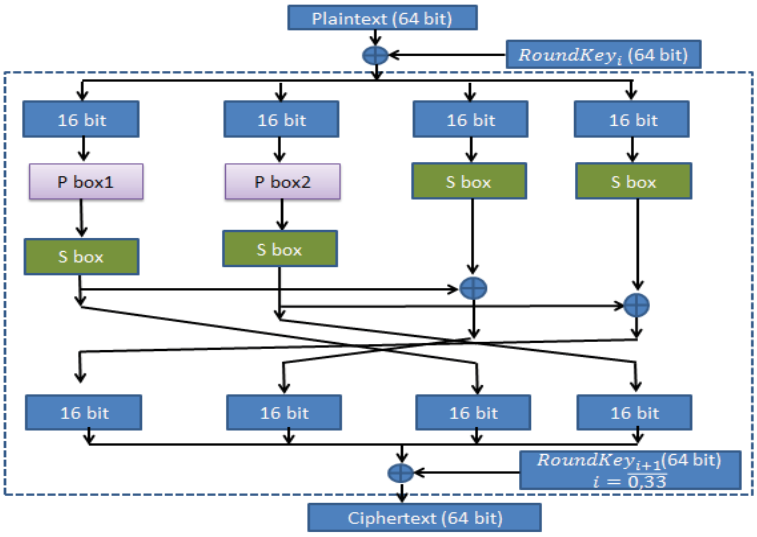

Рис. 1- Схема алгоритма шифрования

Процесс шифрования состоит из 4 этапов:

1 этап. В первой процедуре выполняется операция наложения (суммирования) раундового ключа по модулю 2 на блок открытого текста. Далее входной блок разбивается на 4 части (подблоки) по 16 бит, которые служат входами для следующих этапов.

2 этап. 1-й и 2-й входные подблоки в соответствии со схемой проходят преобразования P-box1(таблица 1), P-box2 (таблица 2), затем эти подблоки проходят через 4-битный S-box согласно схеме (рисунок 1).

3 этап. 3-й и 4-й входные подблоки, согласно схеме, проходят через 4-битный S-box (таблица 3) и затем выполняется операция XOR с результатами подблоков 1 и 2 соответственно, которые в свою очередь прошли преобразования S-box.

4 этап. Результаты этапов 2 и 3 объединяются согласно схеме и выполняется операция наложения (суммирования) раундового ключа по модулю 2.

Преобразование P-box. В 1 блоке, в преобразовании P-box 1 каждый бит распределяется в соответствии с таблицей 1, а во 2 блоке в преобразовании P-box 2 каждый бит перемещается в соответствии с таблицей 2.

Таблица 1- Преобразования P-box1

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	3	7	8	6	11	0	5	14	10	13	2	1	15	4	12	9

Таблица 2 - Преобразования P-box2

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	12	3	13	11	0	8	5	6	9	4	14	7	2	1	15	10

Преобразование S-box. Представим входные 16 бит следующим образом: $a_0a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}$.
Затем формируются каждые 4 бита следующим образом: $m_0 = a_0a_1a_2a_3,\ m_1 = a_4a_5a_6a_7,\ m_2 = a_8a_9a_{10}a_{11},\ m_3 = a_{12}a_{13}a_{14}a_{15}$ каждый $m_i,\ i = \overline{0,3}$. Согласно таблице 3, преобразованный текст проходит через 4-битный S-блок, и новые полубайты, полученные после прохождения каждого S-блока, заменяются, как показано на рис. 2.

Таблица 3 - График замены S-box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7

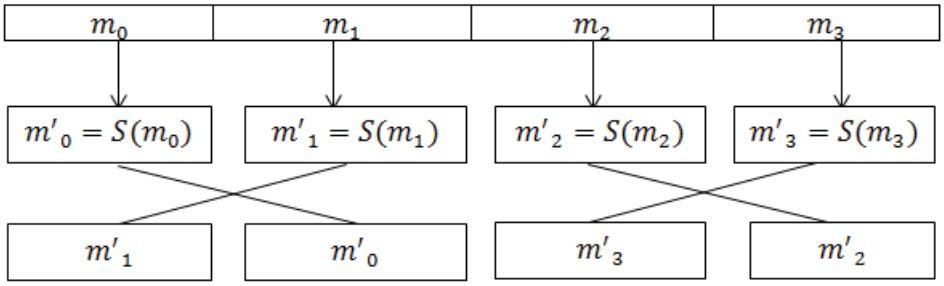

Рис. 2 - Процесс преобразования S-box

Алгоритм генерации раундовых ключей. Раундовые ключи находятся по базовой длине ключа 80 бит согласно алгоритму, представленному на рис. 3. Преобразования, используемые здесь, блоки P-box1, P-box2 и 4-битные S-box такие же, как в алгоритме шифрования.

Лавинный эффект – важное криптографическое свойство для шифрования. Лавинный эффект в преобразовании проявляется в значительном «лавинном» изменении битов в выходном значении преобразования при малом изменении битов во входном значении преобразования по сравнению с исходным значением. Для характеристики степени лавинного эффекта в криптографическом преобразовании определяется и используется лавинный параметр – численное значение отклонения вероятности изменения бита в выходной последовательности при изменении бита во входной последовательности от требуемого значения вероятности, равной 0,5. Если малые изменения в открытом тексте приводят к малым изменениям в зашифрованном тексте, то это позволяет злоумышленнику сузить пространство ключей или область поиска открытого текста [5]. Для лавинного критерия значение лавинного параметра определяется формулой $\varepsilon = |2k_i - 1|$,

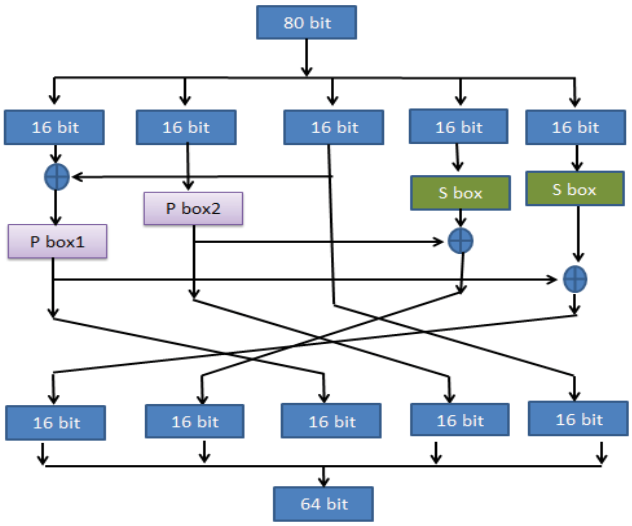

Рис. 3 - Алгоритм генерации раундовых ключей

где i – номер изменяемого бита во входном значении, k_i– вероятность изменения половины битов в выходном значении при изменении i-го бита во входном значении по сравнению с выходным значением при исходном (неизмененном) входном значении.

В практических примерах случайный открытый текст выбирается длиной 64 бит. После инверсии битов в каждой позиции получаются 64 новых открытых текстов, которые зашифровываются. Вычисляются вероятности k_i между полученными шифртекстами и исходным шифртекстом.

При этом, чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании. Результаты анализа по открытому тексту описанного алгоритма приведены в таблице 4.

Среднее значение ε равно 0,08, т.е. рассматриваемый алгоритм удовлетворяет требованиям лавинного критерия.

Таблица 4 - Анализ лавинного эффекта по открытому тексту для разработанного алгоритма

i	k_i	*i*	k_i	*i*	k_i	*i*	k_i	*i*	k_i	*i*	k_i	*i*	k_i	*i*	k_i
1	0,56	9	0,59	17	0,39	25	0,5	33	0,42	14	0,46	49	0,51	57	0,51
2	0,48	10	0,54	18	0,47	26	0,53	34	0,48	42	0,42	50	0,42	58	0,4
3	0,48	11	0,46	19	0,51	27	0,47	35	0,55	43	0,53	51	0,43	59	0,47
4	0,43	12	0,5	20	0,57	28	0,47	36	0,43	44	0,42	52	0,45	60	0,47
5	0,57	13	0,45	21	0,46	29	0,40	37	0,47	45	0,5	53	0,51	61	0,51
6	0,46	14	0,45	22	0,54	30	0,55	38	0,56	46	0,48	54	0,5	62	0,57
7	0,5	15	0,54	23	0,47	31	0,57	39	0,45	47	0,42	55	0,48	63	0,54
8	0,48	16	0,51	24	0,53	32	0,57	40	0,46	48	0,60	56	0,5	64	0,41

Заключение. Если криптографический алгоритм не обладает лавинным эффектом в достаточной степени, то злоумышленник может получить представление о входной информации, основываясь на выходной информации.

Чем меньше значение лавинного параметра, тем сильнее лавинный эффект в преобразовании. Таким образом, рассмотренный алгоритм демонстрирует свойства достаточно сильного лавинного эффекта. Лавинный эффект оказывается явно заметным уже после первого раунда шифрования. Исследование свойств данного алгоритма продолжаются, полученные результаты будут изложены в последующих работах.

Благодарность. Исследовательская работа выполнена в рамках проекта грантового финансирования AP09259570 «Разработка и исследование отечественного легковесного алгоритма шифрования при ограниченности ресурсов» Министерства образования и науки Республики Казахстан.

Список использованных источников

1. Kapalova N.A., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform, Cogent Engineering (2020), 7:1788292, ISSN 2331-1916, V. 7. – P. 1-12.

2. Manifavas C., Hatzivasilis G., Fysarakis K., Rantos K. Lightweight Cryptography for Embedded Systems - A Comparative Analysis, SETOP'2013.

3. Жуков А.Е., Легковесная криптография (Часть 1), Вопросы кибербезопасности №1(9) – 2015, Стр. 26-43.

4. Panasenko S., Smagin S. Lightweight Cryptography: Underlying Principles and Approaches. International Journal of Computer, Theory and Engineering, Vol. 3, No. 4, August 2011, pp. 516-520.

5. Капалова Н.А., Алгазы К.Т., Хомпыш А., Исследование разработанного алгоритма на основе преобразования EM по критерию «лавинного эффекта», Вестник Академия транспорта и коммуникаций им. М. Тынышпаева. – Алматы, 2020. – №3 (114). – 284-292б.