МРНТИ 81.93.29
УДК 004.056.5

https://doi.org/10.51889/2021-3.1728-7901.14

*Н.А. Капалова[1], А. Хаумен[1]**

[1]Институт информационных и вычислительных технологий, Алматы, Казахстан
**email: haumen.armanbek@gmail.com*

ДИНАМИЧЕСКИЕ ТАБЛИЦЫ ПОДСТАНОВОК СИММЕТРИЧНЫХ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация

В работе рассматриваются нелинейные преобразования известных симметричных блочных алгоритмов, таких как AES, Кузнечик, SM4, BelT и Калина. Исследуются свойства нелинейности описанных таблиц подстановок с вычислением соответствующих значений. На основе свойства нелинейности предлагается метод генерации динамической таблицы подстановок. Целью данного метода является генерация динамических таблиц подстановок (S-блоков), изменяющихся в зависимости от значений некоторого параметра, получаемых из секретного ключа алгоритма. Учитывая, что при линейном и дифференциальном криптоанализах используются известные таблицы подстановок, главным преимуществом нового метода является то, что S-блоки случайно зависят от ключа и неизвестны. Также были проведены численные эксперименты для реализации данного метода. Полученные динамические таблицы подстановок были исследованы на нелинейность и результаты сравнивались с исходными значениями нелинейности этих же таблиц подстановок.

Ключевые слова: алгоритм шифрования, таблица подстановок, динамический S-блок, нелинейное преобразование.

Аңдатпа

*Н.А. Капалова[1], А. Хаумен[1]**

[1]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан

СИММЕТРИЯЛЫ БЛОКТЫҚ ШИФРЛЕУ АЛГОРИТМДЕРДІҢ ДИНАМИКАЛЫҚ АЛМАСТЫРУ КЕСТЕЛЕРІ

Бұл жұмыста AES, Кузнечик, SM4, BelT және Калина сияқты симметриялық блоктық шифрлеу алгоритмдерінің сызықтық емес түрлендірулері қарастырылады. Аталған алгоритмдердің алмастыру кестелерінің қысқаша түсіндірмесі беріледі. Сондай-ақ, осында сипатталған алмастыру кестелерінің сызықты емес қасиеті туралы сөз қозғалып, сызықсыздықтың мәні есептелініп көрсетіледі. Алмастыру кестелерінің сызықсыздық қасиеті негізінде динамикалық алмастыру кестелерін жасаудың бір тәсілі құрастырылып, келтірілген. Бұл ұсынылып отырған тәсілдің мақсаты – алгоритмнің құпия кілттінің негізінде алынған параметрге байланысты өзгеріп отыратын динамикалық алмастыру кестесін құрастыру болмақ. Сондай-ақ, осы тәсілді жүзеге асыру бойынша зерттеу, тәжірибелік жұмыстар жүргізілді. Тәжірибе барысында жасалынған динамикалық алмастыру кестелері сызықсыздыққа зерттелініп, алынған мәндердің алмастыру кестелерінің бастапқы сызықсыздық мәндерімен салыстырылып, талдау жұмыстары жүргізілді.

Түйін сөздер: шифрлеу алгоритмі, алмастыру кестесі, динамикалық S-блоктар, сызықтық емес түрлендіру.

Abstract

DYNAMIC SUBSTITUTION BOXES OF SYMMETRIC BLOCK ENCRYPTION ALGORITHMS

*Kapalova N.A. [1], Haumen A. [1]**

[1]Institute of Information and Computational Technologies, Almaty, Kazakhstan

The paper deals with nonlinear transformations of well-known symmetric block algorithms such as AES, Kuznyechik, SM4, BelT, and Kalyna. A brief description of the substitution boxes for these algorithms is given. The properties of nonlinearity of the described substitution boxes are investigated with the calculation of the corresponding values. Based on the property of nonlinearity, a method for generating a dynamic substitution box is proposed.The purpose of this method is to generate dynamic substitution boxes (S-boxes) that change depending on the values of some parameter obtained from the secret key of the algorithm.Considering that linear and differential cryptanalysis uses known substitution boxes, the main advantage of the new method is that S-boxes are randomly key-dependent and unknown.Experiments werealso carried out to implement this method. The resulting dynamic substitution boxes were tested for nonlinearity and the results were compared with the original nonlinearity values of the same substitution boxes.

Keywords: encryption algorithm, substitution box, dynamic S-box, nonlinear transformation.

Введение

В эпоху развития информационных технологий симметричные блочные алгоритмы шифрования являются основным средством обеспечения защиты информации при обработке их в современных информационно-телекоммуникационных системах. Степень надежности криптографической защиты информации и защищенность информационно-телекоммуникационной системы зависят от уровня стойкости и свойства используемого в системах алгоритма шифрования. Благодаря высокой эффективности и низкой сложности реализации, симметричные блочные алгоритмы широко используются для защиты данных[1]. Великий ученый К.Шеннон сформулировал в своих ключевых трудах по теории шифрования, каким условиям должен удовлетворять стойкий блочный шифр [2]. Стойкие шифры должны обладать следующими свойствами:

– рассеивание (diffusion): это свойства алгоритма, при котором влияние одного бита открытого текста распространяется на большое количество битов шифротекста, скрывая статистические характеристики между зашифрованным текстом и исходным текстом.

– перемешивание (confusion): это свойство алгоритма скрывать зависимости между исходным и зашифрованным тесктом. Если преобразование достаточно хорошо "перемешивает" биты исходного текста, то получаемый шифртекст не содержит никаких статистических и функциональных закономерностей. Перемешивание обеспечивает как можно более сложную зависимость ключа и зашифрованных текстов и усложняет задачу получения информации о секретном ключе.

Для обеспечения требований к блочным шифрам, сформулированных К.Шенноном, в современных блочных алгоритмах шифрования используются различные преобразования: линейные и нелинейные. В данной работе речь идет о нелинейных преобразованиях, используемых в симметричных блочных алгоритмах.

Нелинейное преобразование в симметричных блочных алгоритмах шифрования

Нелинейное преобразование необходимо для каждого современного алгоритма шифрования. Доказано, что оно является сильным криптографическим примитивом против линейного и дифференциального криптоанализа. Нелинейные преобразования в современных симметричных блочных алгоритмах (СБА) реализованы в виде таблиц подстановки (s-блоков)[3].

Учитывая, что большинство известных алгоритмов шифрования (AES, Кузнечик, Калина, BelT и др.) для добавления раундовых ключей к блоку данных используют единственную линейную операцию – xor (сложение по модулю 2), то табличные подстановки (*S*-блоки) оказываются единственным примитивом, которые определяют нелинейность преобразования и степень егостойкости к различным видам атак. Количество раундов симметричных алгоритмов шифрования вычисляется на основе исследования стойкости к известным видам криптографических анализов при условии заданных свойств нелинейной табличной замены [4]. Многие поточные алгоритмы, криптографические хэш-функции, генераторы псевдослучайных последовательностей построены на базе блочных шифров или их конструктивных элементов. Таким образом, криптографическая стойкость большинства современных СБА в значительной степенизависит от свойств выбранных *S*-блоков.

Основными нелинейными преобразованиями современных алгоритмов шифрования являются табличные подстановки. Для определения стойкости алгоритмов шифрования существует различные критерии для S-блоков. Несмотря на множество существующих решений вобласти симметричных блочных алгоритмов шифрования, актуальным остаётся вопрос по разработке табличных подстановок (S-блоков), применение которых в криптографических алгоритмах обеспечивает хорошую защиту от всех видов криптоатак [4].

Подстановки, применяемые вкриптографических алгоритмах, должны удовлетворять следующим критериям [5]:

a) максимизация нелинейности подстановки;
b) минимальная степень должна равняться 3;
c) минимизация максимального значения таблицы дифференциалов.

В данной работе рассмотрены свойства нелинейности известных алгоритмов шифрования таких, как AES [6], Кузнечик [7], SM4 [8], BelT [9], Калина [10] и другие, были вычислены значения нелинейности S-блоков этих алгоритмов с помощью компьютерной программы. Программа реализована на языке Python 3. С помощью разработанной программы вычислены и

проанализированы значения нелинейности S-блоков известных алгоритмов шифрования (формула (1)).

Пусть $S = (f_0, f_1, \dots, f_{m-1})$ – некоторая $n \times m$ подстановка, где f_i–булева функция от n переменных. Обозначим через g_iмножество всех линейных комбинаций f_i. Тогда нелинейность S равна [11]:

$$NL(S) = \min\left(NL(g_j)\right), 0 < j < 2^m \quad (1)$$

В таблице1 приведены результаты вычисления значения нелинейности S-блоков этих алгоритмов.

Таблица 1. Значения нелинейности алгоритмов

Алгоритмы	*Значение нелинейности*
AES	*112*
Кузнечик	*116*
SM4	*112*
BelT	*110*
Калина – S0	*112*
Калина – S1	*110*
Калина – S2	*110*
Калина – S3	*112*

Динамические S-блоки

В последнее время опубликовано ряд научных работ по созданию динамических S-блоков алгоритма шифрования. В работах [3, 12, 13] рассматриваются методы динамического создания S-блоков различными способами. В [3] предложены динамические S-блоки на основе S-блока алгоритма шифрования AES. Динамическое генерирование S-блоков с помощью генераторов псевдослучайных последовательностей описано в публикациях [12, 13].

В данной работе авторами представлен разработанный ими метод создания динамических S-блоков на основе известных и проверенных S-блоков. Идея данного метода заключается в генерации динамических S-блоков, меняющихся при каждом изменении секретного ключа. Основное преимущество данного подхода состоит в том, что S-блоки случайны, зависят от ключа и заранее неизвестны, поскольку как линейный, так и дифференциальный криптоанализ требуют известных S-блоков.

Для начала был выбран S-блок алгоритма AES. Из мастер ключа шифрования с помощью различных преобразований получаем один байт. Например, путем суммирования всех байтов мастер ключа по модулю 2. Этот же байт будет использоваться как константа в следующем аффинном преобразовании:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}$$

где a_i – биты байта S-блока, c_i–биты константы (полученный байт из мастер ключа), b_i – биты нового байта S-блока.

В итоге данного аффинного преобразования получаем новый S-блок, отличающийся от исходного S-блока. Полученный S-блок и будет использоваться в процессе нелинейного преобразования алгоритма шифрования. В ходе исследования выявлено, что после такого преобразования свойства нелинейности S-блоков сохраняются. Результаты экспериментов приведены в таблице 2.

Также были исследованы различные свойства динамически созданных S-блоков с помощью специальных программ, разработанных в лаборатории информационной безопасности.

В таблице 3 представлены результаты исследования динамического S-блока алгоритма AES, полученный при значении C = 36, 109 и 221.

Таблица 2. Значения нелинейности алгоритмов после преобразования

Алгоритм	*Первоначальное значение нелинейности*	*Значение нелинейности после преобразования*
AES	*112*	*112*
Кузнечик	*116*	*116*
SM4	*112*	*112*
BelT	*110*	*110*
Калина-S0	*112*	*112*
Калина-S1	*110*	*110*
Калина-S2	*110*	*110*
Калина-S3	*112*	*112*

Таблица 3. Сравнение результатов тестов для S-блоков

Свойства	*S-блок-1*	*S-блок-2*	*S-блок-3*
Значения параметра C	*36*	*109*	*221*
Вес Хэмминга	*128*	*128*	*128*
Сбалансированность	*True*	*True*	*True*
Вес Хэмминга - Minimum	*128*	*128*	*128*
Расстояние Хэмминга	*128*	*128*	*128*
Нелинейность(min)	*112*	*112*	*112*
Нелинейность(max)	*144*	*144*	*144*
Значение корреляции (min)	*-32*	*-32*	*-32*
Значение корреляции (max)	*32*	*32*	*32*
|AC| min	*-32*	*-32*	*-32*
|AC|max	*32*	*32*	*32*
| SSI |min	*133120*	*133120*	*133120*
| SSI |max	*133120*	*133120*	*133120*
SAC	*False*	*False*	*False*
Критерий распространения	*нет*	*нет*	*нет*
CI	*нет*	*нет*	*нет*
t-устойчивость	*нет*	*нет*	*нет*

Полученный S-блок будет использоваться при шифровании. Для каждого процесса шифрования будет свой S-блок, значения которого заранее неизвестны. Это свойство, в свою очередь, затрудняет как дифференциальный, так и линейный криптоанализ.

При расшифровании используется обратная таблица замены. Обратный S-блок генерируется тоже динамически из созданного основного S-блока. При этом нет необходимости сохранять обратный S-блок.

Заключение

Полученные результаты будут использоваться при разработке алгоритма шифрования данных, который разрабатывается в Лаборатории информационной безопасности Института информационных и вычислительных технологий Комитета науки Министерства образования и науки Республики Казахстан. В дальнейшем как продолжение данной работы, будут исследованы другие крипографические свойства динамически генерируемых S-блоков.

Благодарность

Научно-исследовательская работа выполнена в рамках проекта № AP09259570 «Разработка и исследование отечественного легковесного алгоритма шифрования при ограниченности ресурсов».

Список использованной литературы:

1 Горбенко И.Д., Долгов В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И., Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования. // Известия южного федерального университета. Технические науки, № 1, том 76, с.183-189, 2007.

2 Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333–369

3 Kazlauskas K. and Kazlauskas J., "Key-dependent S-box generation in AES block cipher system," Informatica, vol. 20, pp. 23-34, 2009.

4 Олейников Р.В., Казимиров А.В. Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств // Вісн. Харк. нац. ун-ту. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління.Х., 2010. – № 925. – С. 79–86.

5 Горбенко І. Д., ГорбенкоЮ. І. Прикладна криптологія,. – Х. : Форт, 2012. – 870с.

6 Specification for the Advanced Encryption Standard (AES) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (дата обращения 02.05.2021)

7 Криптографическая защита информации Блочные шифры – ГОСТ Р 34.12–2015. – URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 02.05.2021)

8 SMS4 Encryption Algorithm for Wireless Networks. Translated and typeset by Whitfield Diffie of Sun Microsystems and George Ledin of Sonoma State University, 15 May 2008

9 Агиевич С.В., Галинский В.А., Микулич Н.Д., Харин Ю.С. Алгоритм блочного шифрования BelT/ Управление защитой информации, том 6, №4, 2002. – с.407-412.

10 Кузнецов О.О., Иваненко Д.В., Колованова Е.П. Моделирование перспективного блочного шифра «Калина» // Прикладна радіоелектроніка: наук.-техн. журнал. – 2014. – Том 13. – № 3. – С. 201–207.

11 Казимиров А.И. Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов. // Дисс. … канд. тех.наук. Харьковский нац.университет радиоэлектроники, 2013.

12 B. B. Cassal-Quiroga, E. Campos-Cantón, "Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map", Mathematical Problems in Engineering, vol.2020, Article ID2702653,12 pages, 2020. https://doi.org/10.1155/2020/2702653

13 Jiqiang Lu, Hwajung Seo, "A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design" Security and Communication Networks, vol. Article ID1457419, 26 pages, 2020. https://doi.org/10.1155/2020/1457419

References

1 Gorbenko I.D., Dolgov V., Olejnikov R.V., Ruzhencev V.I., Mihajlenko M.S., Gorbenko YU.I., (2007) Razrabotka trebovanij i princip proektirovaniya perspektivnogo simmetrichnogo blochnogo algoritma shifrovaniya [Development of requirements and the design principle of a promising symmetric block encryption algorithm], Izvestiya yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki [Southern Federal University news, Technical sciences], Vol.76, №1, P.183-189. [in Russian].

2 Shennon K. Raboty po teorii informacii i kibernetike (1963) [Works on information theory and cybernetics], Moscow., IL, P.333-369 [in Russian].

3 Kazlauskas K. and Kazlauskas J., "Key-dependent S-box generation in AES block cipher system," Informatica. 2009, vol. 20, pp. 23-34.

4 Olejnikov R.V., Kazimirov A.V. (2010). Vybor S-blokov dlya simmetrichnyh kriptograficheskih algoritmov na osnove analiza algebraicheskih svojstv [Selection of S-blocks for symmetric cryptographic algorithms based on the analysis of algebraic properties], Vesn. Hark. nac. un-tu. Ser. Matematichne modelyuvannya. informacijni tekhnologii. Avtomatizovani sistemi upravlinnya [Kharkiv National University news, Mathematical modeling, Information technologies, Automated control systems]. Kharkiv., №925. P.79-86. [in Russian].

5 Gorbenko I. D., Gorbenko YU. I. (2012) Prikladna kriptologiya [Applied cryptography]. Kharkiv.: Fort,. 870. [in Russian].

6 Specification for the Advanced Encryption Standard (AES) [Electronic resource]. Available at: URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (Accessed 02.05.2021)

7 Kriptograficheskaya zashchita informacii Blochnye shifry GOST R 34.12-2015 [Cryptographic protection of information, Block ciphers] [Electronic resource]. Available at: URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (Accessed: 02.05.2021) [in Russian].

8 SMS4 Encryption Algorithm for Wireless Networks. (2008) Translated and typeset by Whit field Diffie of Sun Microsystems and George Ledin of Sonoma State University.

9 Agievich S.V., Galinskij V.A., Mikulich N.D., Harin YU.S. (2002) Algoritm blochnogo shifrovaniya BelT [BelT Block Encryption Algorithm] Upravlenie zashchitoj informacii [Information security management], Vol. 6, №4, .407-412. [in Russian].

10 Kuznecov O.O., Ivanenko D.V., Kolovanova E.P. (2014). Modelirovanie perspektivnogo blochnogo shifra «Kalina» [Modeling of a promising block cipher «Kalina»], Prikladna radioelektronika: nauk.-tekhn. zhurnal [Applied radioelectronics: scientific and technical journal]. Vol. 13. №3. 201-207. [in Russian].

11 Kazimirov A.I. (2013) Metody i sredstva generacii nelinejnyh uzlov zameny dlya simmetrichnyh kriptoalgoritmov [Methods and means of generating nonlinear replacement nodes for symmetric crypto algorithms]. Dissetraciya na soiskanie uchenoj stepeni kanditata tekhnicheskih nauk. Har'kovskij nacional'nyj universitet radioelektroniki [Candidate's thesis. Kharkiv, [in Russian].

12 Cassal-Quiroga B. B., Campos-Cantin E.. (2020) Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map, Mathematical Problems inEngineering, vol., Article ID2702653,12 pages https://doi.org/10.1155/2020/2702653

13 *Jiqiang Lu, Hwajung Seo. A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design, Security and Communication Networks, vol.2020, Article ID1457419, 26 pages, 2020. https://doi.org/10.1155/2020/1457419*