DOI 10.52209/1609-1825_2023_4_478 УДК 004.421

Линейный криптоанализ алгоритма LBC

[1]***АЛГАЗЫ Кунболат Тилеуханулы,*** *PhD, старший научный сотрудник, kunbolat@mail.ru,*
[1]***ХАУМЕН Армиянбек,*** *младший научный сотрудник, haumen.armanbek@gmail.com,*
[1]***ХОМПЫШ Ардабек,*** *научный сотрудник, ardabek@mail.ru,*
[1]***САКАН Кайрат Саканулы,*** *научный сотрудник, kairat_sks@mail.ru,*
[1]*Институт информационных и вычислительных технологий, Казахстан, Алматы, ул. Шевченко, 28,*
**автор-корреспондент.*

Аннотация. *Алгоритмы легковесного шифрования считаются относительно новым направлением в развитии криптографии с закрытым ключом. Такая потребность появилась в результате появления большого количества устройств с небольшой вычислительной мощностью и памятью. LBC – это 64-битный симметричный блочный алгоритм. Он поддерживает 80-битный секретный ключ. Количество раундов – 20. В статье оценена его защищенность от линейного криптоанализа. Результаты исследований выявила хорошие криптографические свойства данного алгоритма. Алгоритм будет применяться для устройств, обладающих малыми аппаратными ресурсами, в информационно-коммуникационных системах, где циркулируют сведения конфиденциального характера, а также крайне необходимо в оперативно приемлемые сроки обмениваться информацией в защищенном виде.*

Ключевые слова: *легковесная криптография, линейный криптоанализ, S-блок, криптостойкость, нелинейность.*

Введение

Линейный криптоанализ является одним из наиболее важных методов анализа криптографических примитивов с симметричным ключом. Линейный криптоанализ фокусируется на линейном приближении между открытым текстом, зашифрованным текстом и ключом. Если шифр ведет себя иначе, чем случайная перестановка для линейного криптоанализа, это можно использовать для создания отличительного признака или даже атаки восстановления ключа путем добавления нескольких раундов. Линейный криптоанализ использовался для анализа многих шифров [1].

Основа линейного криптоанализа [2] – поиск линейного приближения, которое изучает линейную приблизительную связь между набором битов открытого текста и битов зашифрованного текста, т.е. выяснить, какая линейная связь существует между некоторыми битами открытого текста, битами зашифрованного текста и битами неизвестного ключа.

$$A[a_1, a_2, \ldots, a_n] \oplus C[c_1, c_2, \ldots, c_m] = K[k_1, k_2, \ldots, k_l], \quad (1)$$

где $a_1, a_2, \ldots, a_n, c_1, c_2, \ldots, c_m$ и $k_1, k_2, \ldots, k_l$ обозначают фиксированные позиции битов, а уравнение (1) выполняется с вероятностью $p \neq 1/2$ для произвольно заданного открытого текста A, соответствующего шифртекста C и ключа K [2].

Для простых линейных операций, таких как *xor* с ключом или перестановка битов, можно написать очень простые линейные уравнения, которые выполняются с вероятностью единица. Для нелинейных элементов шифра, таких как S-блоки, найти линейные приближения с вероятностью p. При этом для успешного проведения анализа, вероятность уравнений p должна быть как можно дальше удалена от значения 0,5.

Сначала проводится поиск аппроксимации для отдельных операций внутри шифра, затем объединяются в аппроксимации, которые справедливы для одного раунда шифра. Путем соответствующей конкатенации одноразовых аппроксимаций злоумышленник в конечном итоге получает аппроксимацию для всего шифра [3].

Для определения сложности атаки необходимо оценить вероятность линейной характеристики. Линейную аппроксимацию одного раунда можно рассматривать как случайную величину вида $\alpha_1 X_1 \oplus \alpha_2 X_2 \oplus \ldots \oplus \alpha_n X_n \oplus \beta_1 Y_1 \oplus \beta_2 Y_2 \oplus \ldots \oplus \beta_m Y_m$, которая принимает либо значение ноль, либо единицу (в зависимости от битов ключа). Тогда линейная характеристика xor этих случайных величин и вероятность линейной характеристики может быть вычислена с помощью леммы о набегании знаков (лемма 1).

Рассмотрим две независимые случайные величины X_1 и X_2. Отсюда $P(X_i=0)=p_i$ и $P(X_i=1)=1-p_i$ для $i \in \{1, 2\}$. Тогда из независимости X_1 и X_2 следует, что $P(X_1=0,\ X_2=0)=p_1p_2$ и что $P(X_1=1,\ X_2=1)=(1-p1)(1-p_2)$.

Таким образом, $P(X_1 \oplus X_2=0)=p_1p_2+(1-p_1)(1-p_2)$

[4].

Лемма 1. Пусть $X_i (1 \le i \le n)$ – независимые случайные величины, принимающие значения из Z_2 значения которых равны к нулю с вероятностью $\frac{1}{2} + \varepsilon$. Тогда вероятность того, что $X_1 \oplus X_2 \oplus \ldots \oplus X_n = 0$ равна $\frac{1}{2} + \varepsilon$, где $\varepsilon = 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2} \right)$.

Лемма 2. Пусть N – количество заданных случайных открытых текстов и p – вероятность того, что уравнение (1) выполняется, и пусть $\left| p_i - \frac{1}{2} \right|$ достаточно мало. Тогда вероятность успеха алгоритма есть:

$$\int_{-2\sqrt{N}\left|p-\frac{1}{2}\right|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx.$$

Линейный криптоанализ LBC. Алгоритм LBC разработан для шифрования данных блочного типа длиной 64 бит с ключом 80 бит. LBC при шифровании выполняет 20 раундов. Каждый раунд включает в себя 4 вида преобразования: преобразование S, преобразование RL, преобразование L, преобразование K. Подробное описание алгоритма приведено в [5].

В алгоритме шифрования LBC единственным нелинейным этапом является S-блок замены. Все остальные операции линейны и легко поддаются анализу. Построим линейную аппроксимационную таблицу (ЛАТ) для заданного S-блока. В ходе построения таблицы прослеживаются всевозможные комбинации двоичных векторов входа и выхода. Каждую пару векторов используют в качестве маски, которую накладывают на всевозможные пары вход-выход блока замены и определяются следующим соотношением:

$$LAT(\alpha, \beta) \overset{def}{=} \{X \mid X \in Z_2^8, \bigoplus_{i=1}^{8} X[i] \cdot \alpha[i] = \bigoplus_{i=1}^{8} S(X[i] \cdot \beta[i])\},$$

где $\alpha, \beta \in Z_{256}$ и знак умножения обозначает операцию скалярного произведения [6, 7].

В линейной аппроксимационной таблице 1 первый столбец содержит входные маски, а первая строка содержит выходные маски. Если 4-битное линейное уравнение удовлетворяется 0 раз, то можно сделать вывод, что данное 4-битное линейное соотношение отсутствует для этого конкретного S-блока. Если 4-битное линейное уравнение удовлетворяется 16 раз, то также можно сделать вывод, что данное 4-битное линейное соотношение присутствует для этого конкретного 4-битного S-блока. В обоих случаях полная информация передается криптоаналитикам. Результат лучше для криптоаналитиков, если вероятность присутствия или отсутствия уникальных 4-битных линейных уравнений далеко от 1/2 или близко к 0 или 1. Если вероятности присутствия или отсутствия всех уникальных 4-битных линейных отношений равны 1/2 или близко к 1/2, то говорят, что на 4-битном S-блоке трудно произвести линейный криптоанализ. Поэтому результат для криптоаналитика будет лучше, если число восьмерок в таблице меньше. Если количество восьмерок намного больше, чем других чисел в таблице, то говорят, что 4-битный криптографический S-блок более устойчив к линейному криптоанализу [8, 9].

В линейной аппроксимационной таблице ячейки с числами, наиболее удаленными от числа 8, состоят из 12 или 4. Поэтому согласно таблице, эффективные линейные уравнения, необходимые

Таблица 1 – Линейная аппроксимационная таблица для S-блока

Входная маска / Выходная маска	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	8	8	8	10	10	10	10	6	6	10	10	4	12	8	8
2	8	8	4	8	8	12	8	10	10	10	6	10	10	6	10
3	8	12	8	6	6	6	10	8	8	8	12	10	10	6	10
4	8	10	6	12	8	6	6	10	6	8	8	6	6	4	8
5	8	10	6	6	10	8	8	4	8	6	6	6	6	8	12
6	4	10	6	8	8	6	6	8	8	6	6	8	12	10	6
7	4	6	10	6	6	8	8	10	10	8	8	4	8	6	10
8	10	8	6	8	10	8	6	10	12	6	12	6	8	10	8
9	6	8	10	10	8	10	4	8	6	8	10	10	8	10	12
10	10	8	10	12	6	8	10	8	10	4	6	8	10	8	10
11	6	12	10	10	8	10	8	6	12	10	8	8	6	8	6
12	10	6	8	8	6	6	4	4	10	10	8	8	10	6	8
13	6	6	4	10	4	8	10	6	8	8	10	8	6	10	8
14	6	6	8	8	10	10	8	6	8	4	10	10	8	4	6
15	10	10	8	6	4	12	6	8	6	6	8	6	8	8	6

для дальнейшего анализа и вероятность каждого из них равна 3/4, т.е. с наибольшими отклонениями от 1/2:

$$x[3]\oplus s[0]\oplus s[1]=1,$$
$$x[3]\oplus s[0]\oplus s[1]\oplus s[3]=0.$$
$$\ldots$$

Сначала введем обозначение, $k[i,j]$ – элементы раундовых ключей $x[i,j]$ – входные значения блока, $s[i,j]$ и $y[i,j]$ – выходные значения S-блока замены и R_1-функции, где i – номер раунда ($i=1,2,\ldots 20$) и j – номер позиции в блоке, $j=0,1,\ldots,64$. Проведем анализ алгоритма шифрования на семи раундах, так как все выходные биты зависят от всех входных битов после седьмого раунда. Также выбираем выходные уравнение для второго подблока, поскольку в выходном уравнении имеется наименьшее число переменных.

$$Y_1 = SSS(RS\{RS[RS(RS(X_1)\oplus S(X_2))\oplus \oplus SS(X_3)]\oplus SSS(X_4)\}\oplus SSSS(X_1)). \quad (2)$$

Из числа линейных эффективных уравнений, полученных от S-блоков, выберем $x[1]\oplus s[1]=0$. Поскольку входные и выходные переменные участвуют только по одному разу, то это в свою очередь является удобным для дальнейшего анализа. Напишем это уравнение для первого подблока в первом раунде (с учетом, что добавляется ключ): $x[0,1]\oplus k[0,1]\oplus s[0,1]\oplus 1=0$. Вероятность этого уравнения равна 3/4. Далее, согласно схеме шифрования выполняется функция R определим суммы, соответствующие выходному элементу $y[0,1]$. На рисунке показана R-функция для первого подблока.

Согласно схеме R-функции, показанной на рисунке Л1, выходной элемент $y[0,1]$ состоит из суммы первого, восьмого и одиннадцатого элементов, $y[0,1]=s[0,1]\oplus s[0,8]\oplus s[0,11]$. $s[0,8]$ и $s[0,11]$ – 0-й и 2-й выходные биты S-блока замены. В связи с этим, для этих переменных лучше выбрать уравнения $x[1]\oplus x[3]\oplus y[0]=0$ и $x[2]\oplus x[3]\oplus y[2]=1$.

Согласно схеме алгоритма шифрования, переменная $y[0,1]$ объединяется с переменной $y[0,17]$, чтобы получить выходное выражение $y[1,1]$ для первого раунда. Напишем наиболее линейно приближенное уравнение для $y[0,17]$, используя первое выбранное уравнение:

$$y[1,1]=x[0,1]\oplus x[0,8]\oplus x[0,11]\oplus x[0,17]\oplus \oplus k[0,1]\oplus k[0,8]\oplus k[0,11]\oplus x[0,17]. \quad (3)$$

Тогда согласно лемме 1, вероятность данного эффективного уравнения будет равна $\frac{1}{2}+2^2\cdot\left(\frac{1}{2}-\frac{1}{4}\right)^3=\frac{1}{2}+2^{-4}$.

Если используем уравнение (3) для второго раунда, то получим следующее уравнение:

$$y[2,1]=y[1,1]\oplus y[1,8]\oplus y[1,11]\oplus y[1,33]\oplus \oplus k[1,1]\oplus k[1,8]\oplus k[1,11\oplus k[2,33].$$

Учитывая, что каждое $y[1,i]$, $i=1,8,11,33$ состоит из входных переменных в полученном уравнении и под воздействием R-функции, число переменных в первом подблоке удваивается на каждом шаге. Также, в результате проведенного анализа установлено, что в уравнении, полученном после седьмого раунда, участвует 31 переменная. Запишем уравнение линейной аппроксимации выходного элемента для второго подблока в седьмом раунде, используя уравнение (2):

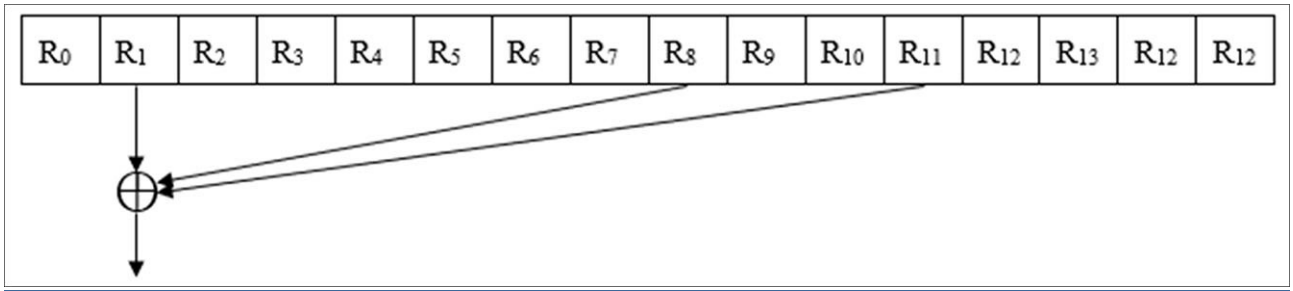
$$y[7,1]\oplus y[6,1]\oplus y[6,8]\oplus y[6,11]\oplus y[6,49]\oplus \oplus k[6,1]\oplus k[6,8]\oplus k[6,11]\oplus k[7,49]=0.$$

Вычисляем отклонение вероятности полученного уравнения от 0,5 (согласно по лемме 1: $\varepsilon=2^{31-1}\cdot\left(\frac{1}{2}-\frac{1}{4}\right)^{31}=2^{-32}$.

Следующий этап заключается в нахождении количества пар открытых текстов и их вероятностей, который позволит нам решить эти уравнения. Для этих целей воспользуемся леммой 2. Для удобстава проведения вычислений, выбираем из таблицы нормальных распределений значение, имеющее одного из наиболее высоких вероятностей, например 0,977. Тогда,

$$-2\sqrt{N}\left|p-\frac{1}{2}\right|\approx -2\Rightarrow N=\left(\frac{1}{0,5+2^{-32}-0,5}\right)^2=2^{64}.$$

Для проведения эффективной атаки с помощью линейного криптоанализа необходимо 2^{64} пары открытого/закрытого текста. В связи с тем, что на вход алгоритма шифрования подаются блоки длинной 64 бита, то максимально возможное количество пар открытого/закрытого текста



Функция R для первого подблока

равно 2^{64}. Таким образом, нет необходимости в проведении линейного криптоанализа для большего числа раундов.

Оценка стойкости нелинейных узлов замены *S*-блока. Применение математического аппарата векторных булевых функций позволяет упростить описание основных элементов симметричных алгоритмов. Такое представление даёт возможность обобщения множества критериев, в том числе и применяемых к подстановкам, одновременно позволяя оценить корреляционные, алгебраические и другие свойства *S*-блоков [9].

Если кратко характеризовать возможности этого подхода, то можно отметить, что его основой является представление *S*-блока в виде композиции компонентных булевых функций с последующим изучением их свойств. Правда, к этим критериям пришлось добавить дополнительные ограничения на максимально допустимые значения элементов таблиц разностей и линейных аппроксимаций, которые, однако, присутствуют и при использовании аппарата булевых функций [8].

В таблице 2 приведены сравнительные характеристики *S*-блоков облегченных шифров. Криптографические характеристики исследованных *S*-блоков получены с помощью специальной программы, разработанной в нашей лаборатории [10].

Выводы. Блочный шифр считается достаточно безопасным для практического использования после того, как он подвергся обширному криптоанализу. Известно, что метод линейного криптоанализа является одним из самых основных критериев оценки криптостойкости алгоритмов блочного шифрования. Для повышения стойкости блочного шифра к линейному и дифференциальному криптоанализу применяют два основных подхода: увеличение числа активных *S*-блоков и использование *S*-блоков с сильными криптографическими свойствами. Результаты линейного криптоанализа показали, что после седьмого раунда шифротексты повторяют свойства случайных подстановок, для эффективной атаки с помощью линейного криптоанализа необходимо 264 пары открытого/закрытого текста. Вероятность нахождения правильных пар очень мала и стремится к сложности полного перебора алгоритма, что позволяет сделать вывод о его стойкости к линейному криптоанализу.

Будут изучены исследовательские работы по алгоритму шифрования LBC и другим методам криптоанализа, а результаты будут опубликованы в журналах.

Данное исследование финансировалось Комитетом науки Министерства образования и науки Республики Казахстан (Грант № AP14870719).

Таблица 2 – Сравнение криптографических характеристик сгенерированной подстановки с S-блоками известных облегченных алгоритмов шифрования

Свойства	S-блоки		
	Present	SIT	LBC
Вес Хэмминга	8	8	8
Сбалансированность	True	True	True
Расстояние Хэмминга	8	8	8
Нелинейность (min)	4	4	4
Нелинейность (max)	12	12	12
Значение корреляции (min)	-8	-8	-8
Значение корреляции (max)	8	8	8
$\|AC\|_{min}$	-16	-8	-8
$\|AC\|_{max}$	16	8	16
$\|SSI\|_{min}$	640	640	640
$\|SSI\|_{max}$	1024	640	640
SAC	False	False	False
Критерий распространения	нет	нет	нет
CI	да	нет	нет
t-устойчивость	да	нет	нет
Циклическая структура S-box	(0; 5; 7), (2; 15; 4), (3; 8; 3), (7; 13; 2),	(0; 3; 2), (1; 15; 2), (2; 14; 2), (4; 5; 2), (6; 11; 2), (7; 12; 2), (8; 13; 2), (9; 10; 2),	(0; 5; 7), (2; 15; 4), (4; 5; 2), (6; 11; 2),

СПИСОК ЛИТЕРАТУРЫ

1. Liu Yu, Liang Huicong, Wang Wei, Wang Meiqin. New Linear Cryptanalysis of Chinese Commercial Block Cipher Standard SM4 // Security and Communication Networks, Hindawi, volume 2017, Article ID 1461520, 10 pages https://doi.org/10.1155/2017/1461520
2. Matsui M. Linear cryptanalysis method for DES cipher Advances in Cryptology – EUROCRYPT'93. Berlin: Springer, 1994. Pp. 386-397.
3. Zhengbin LIU. Differential-linear cryptanalysis of PRINCE cipher [J]. Chinese Journal of Network and Information Security, 2021, 7 (4): 131-140. doi: 10.11959/j.issn.2096-109x.2021072
4. Julia Borghoff. Cryptanalysis of Lightweight Ciphers, 2011, Technical University of Denmark, pp. 60-65. https://backend.orbit.dtu.dk/ws/portalfiles/portal/5456432/phd-thesis_Julia_Borghoff.pdf
5. Nyssanbayeva, Saule, Kapalova, Nursulu, Haumen, Armiyanbek and Suleimenov, Olzhas. The LBC-3 lightweight encryption algorithm // Open Engineering, vol. 12, no. 1, 2022, pp. 570-577. https://doi.org/10.1515/eng-2022-0372
6. Кузнецов А.А., Лисицкая И.В., Исаев С.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс Прикладная радиоэлектроника, 2011, Том 10, № 2, С. 135-140.
7. Ardabek Khompysh, Nursulu Kapalova, Kunbolat Algazy, Dilmukhanbet Dyusenbayev & Kairat Sakan. Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information, Cogent Engineering, no. 9:1, (2022), pp. 1-14. DOI: 10.1080/23311916.2022.2080623
8. Dey S, Ghosh R. A review of existing 4-bit crypto S-box cryptanalysis techniques and two new techniques with 4-bit Boolean functions for cryptanalysis of 4-bit crypto S-boxes. PeerJ Preprints, 2017, 5:e3441v1 https://doi.org/10.7287/peerj.preprints.3441v1
9. Kapalova N., Sakan K. Algazy K. and Dyusenbayev D. Development and study of an encryption algorithm. Computation 2022, 10, 198. – Pp. 1-16. https://doi.org/10.3390/computation10110198.
10. D.S. Duysenbayev, K.T. Algazy, K. Sakan. Study of nonlinear nodes used in symmetric ciphers // International scientific and practical conference, «Actual problems of information security in Kazakhstan», June 11, 2021, Kazakhstan, pp. 34-38.

LBC алгоритмінің сызықты криптоталдауы

[1]***АЛҒАЗЫ Күнболат Тілеуханұлы,** PhD, аға ғылыми қызметкер, kunbolat@mail.ru,*
[1]***ХАУМЕН Армиянбек,** кіші ғылыми қызметкер, haumen.armanbek@gmail.com,*
[1]***ХОМПЫШ Ардабек,** ғылыми қызметкер, ardabek@mail.ru,*
[1]***САҚАН Қайрат Сақанұлы,** ғылыми қызметкер, kairat_sks@mail.ru,*
[1]Ақпараттық және есептеуіш технологиялар институты, Қазақстан, Алматы, Шевченко көшесі, 28,

**автор-корреспондент.*

***Аңдатпа.** Жеңіл салмақты шифрлау алгоритмдері құпия кілтті криптографияның дамуындағы салыстырмалы түрде жаңа бағыт болып саналады. Бұл қажеттілік есептеу қуаты мен жады аз құрылғылардың санының көбеюі нәтижесінде пайда болды. LBC – 64 биттік симметриялық блок алгоритмі. Ол 80 биттік құпия кілтті қолданады. Раундтардың саны – 20. Мақалада оның сызықтық криптоталдауға қарсы қауіпсіздігі бағаланады. Зерттеу нәтижелері бұл алгоритмнің жақсы криптографиялық қасиеттерін көрсетті. Алгоритм шағын аппараттық ресурстары бар құрылғылар үшін, құпия ақпарат айналатын ақпараттық және коммуникациялық жүйелер үшін пайдаланылады, сонымен қатар операциялық қолайлы уақыт шеңберінде қауіпсіз түрде ақпарат алмасу өте қажет.*

***Кілт сөздер:** жеңіл салмақты криптография, сызықтық криптоталдау, S-блок, криптобериктілік, сызықсыздық.*

Linear Cryptoanalysis Algorithm LBC

[1]***ALGAZY Kunbolat,** PhD, Senior Researcher, kunbolat@mail.ru,*
[1]***HAUMEN Armiyanbek,** Junior Researcher, haumen.armanbek@gmail.com,*
[1]***KHOMPYSH Ardabek,** Researcher, ardabek@mail.ru,*
[1]***SAKAN Kairat,** Researcher, kairat_sks@mail.ru,*
[1]Institute of Information and Computational Technologies, Kazakhstan, Almaty, Shevchenko Street, 28,

**corresponding author.*

***Abstract.** Lightweight encryption algorithms are considered a relatively new direction in the development of private key cryptography. This need arose as a result of the emergence of a large number of devices with little computing power and memory. LBC is a 64 bit symmetric block algorithm. It supports 80 bit secret key. The number of rounds is 20. The article evaluates its security against linear cryptanalysis. The research results revealed good cryptographic properties of this algorithm. The algorithm will be used for devices with small hardware resources, in information and communication systems where confidential information circulates, and it is also extremely necessary to exchange information in a secure*

manner within an operationally acceptable time frame.

Keywords: *lightweight cryptography, linear cryptanalysis, S-box, cryptographic strength, non-linearity.*

REFERENCES

1. Liu Yu, Liang Huicong, Wang Wei, Wang Meiqin. New Linear Cryptanalysis of Chinese Commercial Block Cipher Standard SM4 // Security and Communication Networks, Hindawi, volume 2017, Article ID 1461520, pp. 1-11, https://doi.org/10.1155/2017/1461520
2. Matsui M. Linear cryptanalysis method for DES cipher Advances in Cryptology – EUROCRYPT'93. Berlin: Springer, 1994. Pp. 386-397.
3. Zhengbin LIU. Differential-linear cryptanalysis of PRINCE cipher[J]. Chinese Journal of Network and Information Security, 2021, 7 (4), pp. 131-140. doi: 10.11959/j.issn.2096-109x.2021072
4. Julia Borghoff. Cryptanalysis of Lightweight Ciphers, 2011, Technical University of Denmark, pp. 60-65. https://backend.orbit.dtu.dk/ws/portalfiles/portal/5456432/phd-thesis_Julia_Borghoff.pdf
5. Nyssanbayeva, Saule, Kapalova, Nursulu, Haumen, Armiyanbek and Suleimenov, Olzhas. The LBC-3 lightweight encryption algorithm // Open Engineering, vol. 12, no. 1, 2022, pp. 570-577. https://doi.org/10.1515/eng-2022-0372.
6. Kuznecov A.A., Lisickaja I.V., Isaev S.A., Linejnye svojstva blochnyh simmetrichnyh shifrov, predstavlennyh na ukrainskij konkurs Prikladnaja radiojelektronika [Linear Properties of Block Symmetric Ciphers Submitted to the Ukrainian Competition Applied Radio Electronics], 2011, volume 10, no. 2, pp. 135-140.
7. Ardabek Khompysh, Nursulu Kapalova, Kunbolat Algazy, Dilmukhanbet Dyusenbayev & Kairat Sakan. Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information, Cogent Engineering, no. 9:1, (2022), pp. 1-14. DOI: 10.1080/23311916.2022.2080623
8. Dey S, Ghosh R. A review of existing 4-bit crypto S-box cryptanalysis techniques and two new techniques with 4-bit Boolean functions for cryptanalysis of 4-bit crypto S-boxes. PeerJ Preprints, 2017 5:e3441v1 https://doi.org/10.7287/peerj.preprints.3441v1
9. Kapalova N., Sakan K. Algazy K. and Dyusenbayev D. Development and study of an encryption algorithm. Computation 2022, 10, 198. – Pp. 1-16. https://doi.org/10.3390/computation10110198.
10. Duysenbayev D.S., Algazy K.T., Sakan K., Study of nonlinear nodes used in symmetric ciphers // International scientific and practical conference, «Actual problems of information security in Kazakhstan», June 11, 2021, Kazakhstan, pp. 34-38.