Bulletin of L.N. Gumilyov ENU. Mathematics. Computer science. Mechanics series, 2022, Vol. 138, №1, P.6-22
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

МРНТИ: **81.93.29**

С.Е.Нысанбаева [1,2] , К.Т. Алғазы [1] , Қ.С.Сақан [1,2] , А.Хомпыш [1,2] , Д.С.Дүйсенбаев [1]

[1] *ҚР БҒМ ҒК "Ақпараттық және есептеуіш технологиялар институты" Алматы, Қазақстан*
[2] *әл-Фараби атындағы ҚазҰУ Алматы, Қазақстан*
(E-mail: 19kairat78@gmail.com)

CF блокты шифрлау алгоритмі және оны биттік шашырау эффектіне зерттеу

Аңдатпа: Мақалада қазіргі есептеу технологиялардың қарқынмен дамуы кезеңінде мәліметтердің құпиялығын қамтамасыз ету үшін қолданылатын симметриялық блокты шифрлардың маңыздылығы, ерекшеліктері және пайдалану аумағы жайлы айтылады. Осы ретте "Ақпараттық және есептеуіш технологиялар институтының" "Ақпараттық қауіпсіздік зертханасында" жасалынған CF симметриялы блокты шифрлау алгоритмінің құрылымы, оның құпия кілт негізінде раундтың кілттерді жасау механизмі айтылған. Құрылған шифрлау алгоритмінің компьютерлік бағдарламасы жасалды, соның негізінде жұмыс істеу өнімділігі зерделеніп және ашық мәтін мен шифрмәтін арасындағы "лавиндік эффект" қасиеті мен "қатаң лавиндік эффект" қасиеті тексерілді. Алгоритмді аппараттың жүзеге асырылуын оңтайландыру мақсатында сызықтық емес түйін ретінде қарастырылған S-блок ауыстыру түрлендіруі 4x4 биттік өлшемде алынды.

Кілт сөздер: шифрлау алгоритмі, алгоритмнің криптоберіктілігі, "лавиндік эффект" критерийі, "қатаң лавиндік эффект" критерийі.

DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.1

2000 Mathematics Subject Classification: 94-04

1. Кіріспе

Заманауи технологиялардың қарқындап дамуы кезеңінде өзекті болып саналатын бағыттардың ішіндегі ақпараттарды сақтау, сенімді жою мен алмасудағы құпиялылықты жоғарғы дәрежеде қамтамасыз ету үлкен мәселе болып отыр. Осы мақсаттағы ақпараттарды криптографиялық қорғау әдістерінің ішінде симметриялық блокты шифрлау алгоритмдерімен қорғау қазіргі уақытта заманауи ақпараттық және телекоммуникациялық жүйелерде ақпаратты өңдеу барысында құпиялылықты қамтамасыз етудің негізгі сенімді бірден-бір жолы болып табылады [1]. Сол себепті симметриялы блокты шифрлар оның жоғарғы криптоберіктілігіне және жылдамдығына байланысты шифрлаудың басқа кластарымен салыстырғанда кеңінен пайдаланады.

Бүгінгі күндері дамыған елдердің шифрлау алгоритмдері, көбінесе, симметриялық блоктық шифрлардың класына негізделген. Бәрімізге белгілі, симметриялы шифрлар класының қауіпсіздігі голланд криптографы Киркхоффстің өзі аттас принципіне негізделген, оған сәйкес кез-келген симметриялы шифрдың қауіпсіздігі шифрлау алгоритмінің құрылымының құпиялығымен емес, тек оның кілтінің құпиялығында жатыр [2-3].

Ақпараттың қауіпсіздігін қамтамасыз ету үшін криптографиялық жүйелерді қолдану технологиялық дамудың қарқынына да көп байланысты. Қазіргі таңда симметриялы блокты шифрларды қолдану, қолдану шарттары мен мүмкіндіктері саласында үнем жаңарту мен қайта қарауды талап етеді. Әдетте, бұл криптографиялық тұрақтылық,

икемділік және шифрлау жұмысының өнімділігі, сонымен бірге қазір өзекті болып тұрған аппараттық іске асырудағы баға/уақыт тиімділігі бойынша талаптарды қайта қарауға әкеледі [4].

Жасалатын шифрлау алгоритмі қауіпсіздіктің жоғары деңгейін қамтамасыз етуі, тиімді жылдамдықпен жұмыс істеуі, сондай-ақ оның бағдарламалық, аппаратты-бағдарламалық және аппараттық бағытта бізге қажетті деңгейде жүзеге асырыла алуы қажет.

Әлі күнде де блоктық шифр ақпараттың құпиялылығын қамтамасыз етудің маңызды құралы болып табылады. Көбінесе, симметриялы блокты алгоритмдердің құрылымы сызықты және сызықты емес түйіндерден тұрады. Сызықты түрлендірулер – ашық мәтін мәндерін ішінара бір-бірімен барынша жоғары деңгейде араластыру үшін, ал сызықты емес түйіндер – ақпарат пен оның шифрланған нұсқасы арасындағы байланысты барынша қиындату, яғни мейлінше жоғарғы ретті сызықты емес байланыстар орнату [5]. Тәжірибеде сызықты емес түйін мәселесін шешу ретінде S-блок ауыстырулары көп пайдаланылуда. Қазіргі уақытта радиожиілікті сәйкестендіру жүйелері (RFID) сияқты шектеулі ресурстарға ие құрылғылардың қауіпсіздігін арттыруға үлкен мәселелер туындауда. Аз ресурсты құрылғыларда көбінесе 4 биттік S-блок ауыстырулары пайдаланылады. SLIM деп аталатын RFID жүйелеріне арналған жаңа ультражеңіл криптографиялық алгоритм ұсынылған [6]. SLIM алгоритмі Фейстель желісіне негізделген 32 биттік блоктық шифр RFID жүйелері үшін қолайлы, яғни құны мен қауіпсіздігі және энергия қуатын үнемдейтін қасиетке және тамаша өнімділікке ие. Сонымен бірге, 4-биттік S-блок ауыстыруларын қолданатын PRESENT және GIFT сияқты танымал жеңілсалмақты шифрлау алгоритмдерін ауданы мен қуаты жағынан шамамен 40% аз тұтынатын S-блоктар үшін жоғары оңтайландырылған IT сұлбалары жайлы зерттеулер жүргізілген [7].

AUT64 шифрлау алгоритмі қауіпсіздікке сезімтал бірқатар қосымшаларда қолданылатын, мысалы, көлік құралдарының иммобилизациясы сияқты 120 биттік құпия кілті бар 64 биттік блоктық шифры жайлы [8] мақалада зерттеулер жүргізілген. Бұл мақалада блокты шифрлау алгоритмінің толық сипаттамасы және талдауы, онымен байланысты аутентификация хаттамасы, сондай-ақ бірқатар криптографиялық кемшіліктерді қарастырылған. Бұл жоғарғыдағы мақалалар 4-биттік S-блок ауыстыруларын шифрлау алгоритмдерінің құрылымдарында пайдалану әлі де қолданыста өзекті екендігін көрсетіп берді.

Жаңа CF шифрлау алгоритмінде оның бағдарламалы-аппараттық және аппараттық тұрғыда икемді жүзеге асырылу мақсатында және бұл алгоритмді блоктық шифрлар негізінде хеш алгоритмдерін жасауда пайдалануды ойластыра отырып, S-блок ауыстыруларын басқа жолмен іске асыру қарастырылған. Ал, S-блок заманауи блоктық шифрлау алгоритмдерінің құрылысының, соның ішінде кілт жасау алгоритмдерінің де ажырамас бөлігі болып табылады. [9] мақалада Фейстель желісіне таңдалған S-блок механизміне кеңінен тоқталған, Фейстель кілтімен таңдалған S-блок механизмінің жалпыланған нұсқасын жан-жақты қарастырған.

Қазіргі заманғы симметриялық блоктық шифрлау алгоритмдері үшін аналитикалық шабуылдарға криптографиялық төзімділікті бағалау критерийін басшылыққа ала отырып, 4-биттік бірнеше S-блокті белгіленген тәртіппен жұмыс жасататын жаңа CF симметриялық блокты шифрлау алгоримі және оның құрамдас бөлігі CFKey кілт жасау алгоритмі құрылды [10]. Енді сол алгоритмнің құрылымын және әрбір түрлендірулеріне жекелей тоқталып өтейік.

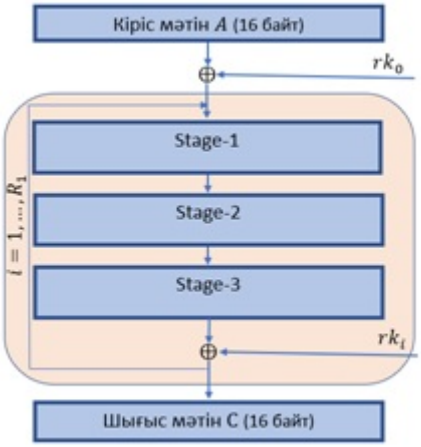
2. Негізгі нәтижелер

2.1. CF шифрлау алгоритмін әзірлеу

2.1.1. CF шифрлау алгоритмінің жалпы сұлбасы

SP желісі негізінде жасалған CF шифрлау алгоритмі ақпараттың қауіпсіздігін криптографиялық тұрғыдан қамтамасыз ету бағытында симметриялық блоктық шифрлау

алгоритмдері класына жатады. Алгоритмнің шифрлау блогінің және кілттің ұзындығы – 128 бит. Алгоритмнің құрамдас бөлігіне сызықтық түрлендірулермен қатар сызықты емес түрлендірулер де кіреді: сызықты түрлендірулер – модуль 2 бойынша биттік қосу және солға қарай циклдық жылжыту операциялары, ал сызықтық емес түрлендірулер ретінде кіріс және шығыс биттерінің көлемі 4 биттен болатын төрт S-блок алмастыруы түрлендіруі қарастырылады. Шифрдың құрылымы ауыстыру-алмастыру желісі (SP-сеть) нұсқасына жатады және шифрлау раундының саны – $R_1 = 4$. Әр шифрлау раунды Stage-1, Stage-2 және Stage-3 түрлендірулерінен тұрады. CF шифрлау алгоритмінің жалпы сұлбасы Сурет-1-де көрсетілген.



Сурет 1 – CF алгоритмі жалпы сұлбасы

Шифрлау жұмысы барысында алдымен раундтық кілтпен ағарту процесі жүргізіледі. Ең бірінші раундтық кілт ретінде негізгі құпия кілтті пайдаланамыз. Әр раундта тізбектей орындалатын Stage-1, Stage-2 және Stage-3 түрлендіруінен кейін алынған шифрмәтінді раундтық кілтпен модуль екі бойынша биттік қосу операциялары орындалып отырады. Соңғы раунд R_1 =4 аяғында 16 байтты шифрмәтін блогін аламыз. Раундтық кілттерді жасау CFKey алгоритмі арқылы іске асырылады, ол жайлы кейінірек тоқталатын боламыз. $A(a_0, a_1, a_2, \ldots, a_{15})$ кіріс мәтін 4x4 өлшемдегі квадрат матрица түрінде келесідегідей ретпен жазып алайық:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_2 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Ескере кететіні, A матрицасының бірінші жазбасында матрица элементтері индекстері кіріс мәтіннің реттік нөмірі бойынша, ал екінші жазбада матрица жолы мен бағанының индексі бойынша жазылған. Матрицаның әр элементі бір байт ретінде қарастырылады. Бұдан әрі әр түрлендірулерге жекелей тоқтала кетейік.

2.1.2. Stage-1 түрлендіруі

Аталған түрлендіру орындалу нәтижесінде берілген A матрицасының өлшеміндегідей жаңа матрица алынады. Stage-1 түрлендіруінің бір ерекшелігі болып шифрлау барысында сызықты және сызықты емес криптографиялық түйіндер қатарласып жұмыс істеуі саналады. Матицаның әр элементтерін есептеу барысында бұл екі түйіндер жұмыс кезінде төмендегідей қадамдармен анықталып, сол элемент үшін екеуі бірінен кейін бірі тізбектесіп орындалып отырады.

1-қадам. Бұл қадам сызықты түйін қадамы. A матрицасы арқылы есептелінетін c_{ij} аралық мәндері матрица құрылымы бойынша солдан оңға, жоғарыдан төмен бағытта есептелініп алынады, мұндағы, $i, j = 0, 1, 2, 3$. c_{ij} аралық мәндері есептелу тәртібі

мынандай: матрицаның i-ші жолындағы төрт элемент пен j-ші бағандағы i мен j қиылысындағы элементтен басқа үш элементтердің модуль екі бойынша биттік қосындысы аталған c_{ij} мәнін береді. Көрсетілген Сурет-2-де мысал ретінде c_{00} аралық мәнін есептеуге қатысатын матрица элементтері белгіленген.

$$c_{00} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Сурет 2 – c_{00} **- элементін есептеу жолы**

2-қадам. Бұл қадам сызықты емес түйін - S-блок ауыстыру операциясынан тұрады. 1-қадамда есептелінген c_{ij} аралық мәні S-блок ауыстырудан өтіп, A матрицасының жаңа мәні ретінде қабылданады, яғни сол орынға жазылады. S-блоктан өткізу реті SBOX процедурасы негізінде жүргізіледі. 1-қадам және 2-қадамнан тұратын Stage-1 түрлендіруін алгебралық түрде мына формуламен жазуға болады:

$$\left.\begin{array}{l} c_{ij} = \oplus \sum\limits_{k=0}^{3} a_{ik} \oplus (\oplus \sum\limits_{k=0,k\neq i}^{3} a_{kj}); \\ a_{ij} = SBOX(c_{ij}); \end{array}\right\} i,j = 0,1,2,3. \qquad (1)$$

мұндағы, c_{ij} – A матрицы арқылы есептелетін аралық мән, SBOX – S-блок ауыстыру процедурасы, $\oplus\sum$ – модуль 2 бойынша биттік қосу операциясы.

2.1.3. SBOX процедурасы

Аталған процедура S-блок ауыстыру операциясын орындайды. Бізге алдынала төрт S_0, S_1, S_2, S_3 блоктары кестемен беріледі, мұндағы $S_i : Z_{2^4} \to Z_{2^4}$, $i = 0, \ldots, 3$. Қарастыратын S_0, S_1, S_2, S_3 ретінде шифрлау алгоритмінде сызықсыздық дәрежесін максимальды етіп алу мақсатына төрт "Алтын S-блоктарды" аламыз және олар Кесте-1-де көрсетілген [11]. Шетелдік ғалымдар M.O. Saarinen және т.б. ғалымдардың еңбектерінде ондаған криптографиялық алгоритмдердің S-блоктарының дифференциалдық және сызықтық қасиеттері бойынша салыстырмалы кестесін құрды және жақсы нәтиже беретін S-блоктарды "Алтын S-блоктар" деп атады. Ұсынылып отырған алгоритмде қолданылған дайын S-блоктар осы S-блоктар топтамасынан алынды [12-14].

Кесте 1 – **Төрт "Алтын S-блоктар"**

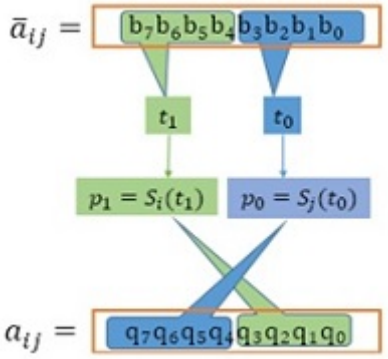
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
$S_0(x)$	0	F	B	8	C	9	6	3	D	1	2	4	A	7	5	E	Serpent, S_3
$S_1(x)$	2	E	F	5	C	1	9	A	B	4	6	8	0	7	3	D	HB-1, S_2
$S_2(x)$	7	C	E	9	2	1	5	F	B	6	D	0	4	8	A	3	HB-2, S_0
$S_3(x)$	4	A	1	6	8	F	7	C	3	0	E	D	5	9	B	2	HB-2, S_1

Ескерту: Serpent - жеңілсалмақты Serpent шифры,
HB-1 - жеңілсалмақты Hummingbird-1 шифры,
HB-2 - жеңілсалмақты Hummingbird-2 шифры.

SBOX процедурасының жұмыс істеу тәртібі төмендегідей тәртіппен анықталады: $a_{ij} = SBOX(\overline{a}_{ij})$. Өңделуге кіріс мән ретінде A матрицасының бір байты $\overline{a}_{ij}$ кіретін болсын. Бұл байттың екілік санау жүйесіндегі жазбасын былай белгілейік: $\overline{a}_{ij} = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)_2$. S-блок ауыстыру операциясы жарты байттар деңгейінде жүргізіледі (ниббл (nybble) немесе тетрада). Сәйкесінше, $\overline{a}_{ij}$ байтының екілік

жазбасын оңжақты жарты байт және солжақты жарты байт деп бөліп алып, төмендегідей белгілеу енгізейік: $t_1 = b_7b_6b_5b_4$, $t_0 = b_7b_6b_5b_4$. Бұдан әрі, осы мәндер арқылы $p_1 = S_i(t_1) = (q_7q_6q_5q_4)_2$, $p_0 = S_j(t_0) = (q_3q_2q_1q_0)_2$ анықтайық. Матрицаның элементінің i мен j индекстері S-блоктың реттік нөмірлерін көрсетеді. Келесіде, i-ші және j-ші S-блоктардан алынған мәндердің екілік жазбасын конкатенация арқылы біріктіреміз. Ескере кететіні, конкатенация кезінде жарты байттар p_0 және p_1 орындарымен алмасады: алынған p_1 - солжақты жарты байт, p_0 - оңжақты жарты байт. Осындай тәртіппен алынған байт шығыс ретінде $(a_{ij})_2 = (p_0)_2 \parallel (p_1)_2$ болып анықталады. SBOX процедурасының жұмыс істеуінің графикалық нұсқасы Сурет-3-те кескінделген.

SBOX процедурасы жұмысына мысал: Бізге $\overline{a}_{32} = 32_{10} = 00100000_2 = 20_{16}$ берілсін. Онда Кесте-1 бойынша мыналарды анықтаймыз $p_1 = S_3(2_{16}) = 1_{16}$, $p_0 = S_2(0_{16}) = 7_{16}$. Бұдан әрі $a_{32} = p_0 \parallel p_1 = 71_{16} = 01110001_2 = 113_{10}$ екенін аламыз. Нәтижесінде $a_{32} = SBOX(32) = 113$ болып шығады.



Сурет 3 – SBOX процедурасы сұлбасы

2.1.4. Stage-2 түрлендіруі

Аталған Stage-2 түрлендіруі екі кезеңнің жиынтығынан тұрады: солға қарай циклдық жылжыту және модуль 2 бойынша биттік қосу (xor операциясы). Бірінші кезеңде Stage-1 түрлендіруінен алынған матрицасының 16 мәні бір өлшемді массив ретпен жазылып алынады $(a_{00}, a_{01}, a_{02}, a_{03}, a_{10}, a_{11}, a_{12}, a_{13}, a_{20}, a_{21}, a_{22}, a_{23}, a_{30}, a_{31}, a_{32}, a_{33})$. Содан әрі, бұл элементтер байт ретінде қабылданып, олардың екілік санау жүйесіндегі жазбасы конкатенация операторы арқылы біріктіріледі: $W = a_{00} \parallel a_{01} \parallel a_{02} \parallel a_{03} \parallel a_{10} \parallel a_{11} \parallel a_{12} \parallel a_{13} \parallel a_{20} \parallel a_{21} \parallel a_{22} \parallel a_{23} \parallel a_{30} \parallel a_{31} \parallel a_{32} \parallel a_{33}$, $|W| = 128$ бит. Осы тізбекке солға қарай 1 бит циклдық жылғыту орындалып, $V = W \lll 1$, алынған тізбек он алты байтты жаңа нәтиже аламыз: $V = b_{00} \parallel b_{01} \parallel b_{02} \parallel b_{03} \parallel b_{10} \parallel b_{11} \parallel b_{12} \parallel b_{13} \parallel b_{20} \parallel b_{21} \parallel b_{22} \parallel b_{23} \parallel b_{30} \parallel b_{31} \parallel b_{32} \parallel b_{33}$. Келесі кезеңде алынған V мен W массивтері xor операциясымен қосылады:

$$A = W \oplus V. \tag{2}$$

Ақырғы алынған нәтиже A матрицасының жаңа элементтері болып солдан оңға, жоғарыдан төмен ретпен жазылады.

2.1.5. Stage-3 түрлендіруі

Stage-3 түрлендіруі құрылымы жағынан жоғарыда көрсетілген Stage-1 түрлендіруіне өте ұқсас. Ол түрлендірудегідей, Stage-3 түрлендіруіндегі матрицасы мәндері бірінші – сызықты, екінші – сызықты емес криптографиялық түйінге жататын екі қадамнан тұратын операциялар арқылы есептелінеді, нәтижесінде жаңа осындай өлшемдегі матрица алынады. Жұмыс істеу тәртібіндегі өзгешелік – жаңа матрица элементтерін есептеудегі бағытта, яғни матрица элементтерін есептеу төменнен жоғарыға дейін, оңнан сол бағытта жүргізіледі. Осы жердегі S-блок ауыстырулары ретінде Кесте-1-де көрсетілген "Алтын S-блоктар" қолданылады. S-блоктар жұмыс реті SBOX процедурасымен жүзеге асырылады.

Әр элементті есептеу барысында қадам-1 мен қадам-2 тізбектеліп жүргізіледі. Есептеу матрицаның a_{33} элементінен бастап, a_{00} элементінен дейін өтеді. Қадам-1 мен қадам-2-ден тұратын есептеуді алгебралық түрде мына формулалармен жүргіземіз:

$$\left.\begin{array}{c} c_{ij} = \oplus \sum\limits_{k=0}^{3} a_{ik} \oplus (\oplus \sum\limits_{k=0,k\neq i}^{3} a_{kj}); \\ a_{ij} = SBOX(c_{ij}); \end{array}\right\} i,j = 3,2,1,0. \tag{3}$$

Аралық мән c_{ij} есептеу кезінде сәйкесінше матрицаның i-ші жолындағы төрт элемент пен j-ші бағандағы үш элементтердің (i-жол мен j-баған қиылысындағы элементтен басқа) модуль екі бойынша биттік қосындысы бойынша жүреді. Сурет-4-де мысал ретінде

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Сурет 4 – c_{33} - элементін есептеуде қатысатын элементтер

c_{33} аралық мәнін есептеуге қатысатын матрица элементтері графиктік түрде көрсетілген. Stage-3 түрлендіруі нәтижесінде аралық шифрланған 16 байтты блок аламыз.

2.1.6. CFKey раундтық кілттерді жасау алгоритмі

Бұл бөлімде 16 байт ұзындықтағы $K(k_0, k_1, k_2, \ldots k_{15})$ құпия кілттен осы ұзындықтағы раундтық кілттерді жасау алгоритмі қарастырылады. Біз K құпия кілтін K_0 раундтық кілт деп ұйғарайық. Раундтық кілттердің жалпы саны осы шифрлау алгоритміндегі R_1 раунд санына сәйкес келеді. Алдымен, $K_0(k_0, k_1, k_2, \ldots k_{15})$ раундық кілтті 4x4 өлшемдегі A квадрат матрицасы түрінде төмендегідей ретпен жазып алайық:

$$A = \begin{pmatrix} k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ k_8 & k_9 & k_{10} & k_{11} \\ k_{12} & k_{13} & k_{14} & k_{15} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

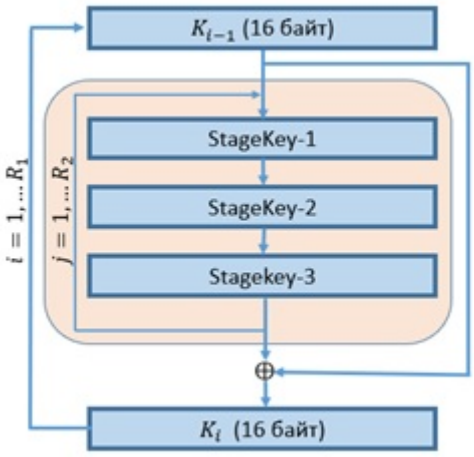
CFKey раундтық кілттерді жасау алгоритмі StageKey-1, StageKey-2 және StageKey-3 түрлендірулерінен тұрады. Ұсынылған кілт жасау алгоритмі жұмысы графикалық түрде Сурет-5-те көрсетілген. Жұмыс істеу тәртібі бойынша аталған CFKey алгоритмі CF шифрлау алгоритмімен өте ұқсас: Stage-1 түрлендіруі StageKey-1 түрендіруімен, Stage-2 түрлендіруі StageKey-2 және Stage-3 түрлендіруі – StageKey-3. Бір ғана айырмашылық – StageKey-2-де. Аталған түрлендіру Stage-2-дағыдай екі операциядан емес, тек бір ғана операциядан тұрады: солға қарай 1 бит циклдық жылжыту операциясы. CFKey алгоритмі Сурет-5-те көрсетілгендегідей келесі K_i раундтық кілтті алу үшін $R_2 = 8$ рет қайталанады, одан соң алынған нәтиже K_{i-1} раундтық кілтімен модуль 2 бойынша биттік қосылады, мұнда $i = 1, \ldots, R_1$ дейін.

2.2. CF шифрлау алгоритмінің бағдарламалық жүзеге асырылуы

Жасалған алгоритмнің бағдарламалық іске асыру жағынан жұмыстар жүргізілді, ол Delphi.7 бағдарламалық тілінде құрылып, алынған нәтижелер шифрлау алгоритмдердің негізгі сипаттамалары жағынан жан-жақты тәжірибелік тұрғыда сараланды. Құрылған бағдарлама төмендегідей функциялардың жұмыс істеуін қамтиды:

– симметриялы раундтық кілттерді жасау;
– файлдарды шифрлау;
– файлдарды кері шифрлау.

Бағдарламаның көмегімен алгоритмнің жұмыс істеу өнімділігі қарастырылды. Шифрлау процесі уақыты 1 Gb ақпаратты шифрлау үшін алдын-ала берілген 16



Сурет 5 – Раундтық кілттерді жасау алгоритмі сұлбасы

байттық ақпарат блогін 67 108 864 рет қайталап есептеу барысында алынды. Осы тәсіл нәтижесінде раунд саны $R_1 = 4$ болғанда, Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz 3.19 GHz процессорі негізінде 1 Gb ақпаратты 1 минут 23 секундта жабады. Кері шифрлау процесіне де осы көрсеткішке шамалас уақыт жұмсалды.

2.3. Әзірлеген алгоритмді қауіпсіздікке талдау

2.3.1. CF шифрлау алгоритмінің биттік шашырауын (лавиндік эффект) зерттеу

Шифрлау алгоритмін жобалау кезінде жасалатын шифр биттік шашырау әсері (лавиндік эффект) критерийін қанағатандыруы керек. Биттік шашырау әсері – шифрлау үшін маңызды криптографиялық қасиет. Бұл қасиет кіріс мәтіндегі немесе кілттегі биттердің аз мөлшердегі өзгерісі шифрмәтіннің шығыс биттерінің қажетті мөлшерде өзгеруіне әкелетінін білдіреді. Биттік шашырау әсерін зерттеу, әдетте, блоктық шифрларға қолданылады. Егер алгоритм қажетті дәрежеде биттік шашырау әсерімен қамтамасыз етілмесе, онда криптоталдаушы шығыс биттер негізінде кіріс биттер туралы ақпарат алуға мүмкіндік алады [11, 12].

Биттік шашырау әсері критерийі үшін биттік шашырау әсері параметрінің мәні мына формуламен анықталады: $\varepsilon_\alpha = |2k_i - 1|$, мұнда, i – кіріс мәндегі өзгертілген биттің нөмірі, k_i – бастапқы (өзгермейтін) кіріс мәнін шығыс мәнімен салыстырғанда кіріс мәніндегі i-ші бит өзгерген кезде шығыс мәніндегі биттердің жартысына жуығының өзгеру ықтималдығы.

CF алгоритмінің биттік шашырауын зерттеу нәтижелерін бағдарлама көмегімен алдық. Егер бір-бірінен тек 1 бит ғана өзгеше екі ашық мәтінді қарастырсақ, онда осы екі ашық мәтін шифрмәтіндері тіпті 1-ші раундтан кейінен-ақ бір-бірінен өзгеше болатынын байқаймыз. Бұл өзгерісті әрбір 1-ден 128-ге дейінгі жеке-жеке өзгерген биттер үшін төмендегі Кесте-2-ден немесе Сурет-6-дан көруге болады.

Өздеріңіз байқағандай, 1-ші раундтан кейін биттік шашырау қанағаттанарлық дәрежеде, ал енді шифрлау алгоритмінің толық 4-ші раундынан кейін де осындай көрсеткіш көрсетуі осыдан-ақ белгілі.

2.3.2. Қарастырылған S-блоктардың қатаң лавиндік эффекті қасиетіне зерттеу

Енді біз қарастырған төрт S-блоктарға қатысты қатаң лавиндік эффектіні зерттейік. Қатаң лавиндік критерийі (SAC) S-блоктарды бағалауда негізгі критерийлердің бірі болып табылады. Ол дифференциалды криптоталдауға төзімділікті сипаттайтын S-блоктарды синтездеу процесінде кеңінен қолданылады [17]. Бәрімізге мәлім, бульдік функцияларды S-блоктар құрылымының бөлігі ретінде қарастыруға болады. SAC-ті қанағаттандыратын

Кесте 2 – Биттік шашырау критерийі

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	0,49	17	0,49	33	0,44	49	0,55	65	0,5	81	0,47	97	0,51	113	0,46
2	0,48	18	0,5	34	0,47	50	0,51	66	0,46	82	0,5	98	0,45	114	0,53
3	0,54	19	0,45	35	0,57	51	0,5	67	0,53	83	0,46	99	0,52	115	0,43
4	0,48	20	0,5	36	0,54	52	0,54	68	0,49	84	0,53	100	0,57	116	0,55
5	0,46	21	0,53	37	0,48	53	0,53	69	0,47	85	0,47	101	0,5	117	0,39
6	0,47	22	0,42	38	0,57	54	0,49	70	0,53	86	0,5	102	0,46	118	0,54
7	0,49	23	0,42	39	0,5	55	0,46	71	0,45	87	0,48	103	0,57	119	0,53
8	0,45	24	0,46	40	0,5	56	0,55	72	0,53	88	0,53	104	0,47	120	0,50
9	0,49	25	0,53	41	0,57	57	0,5	73	0,42	89	0,45	105	0,52	121	0,48
10	0,53	26	0,46	42	0,46	58	0,51	74	0,46	90	0,46	106	0,46	122	0,50
11	0,56	27	0,46	43	0,5	59	0,47	75	0,46	91	0,52	107	0,52	123	0,52
12	0,51	28	0,48	44	0,46	60	0,42	76	0,46	92	0,46	108	0,47	124	0,46
13	0,51	29	0,50	45	0,5	61	0,55	77	0,55	93	0,53	109	0,45	125	0,5
14	0,53	30	0,5	46	0,53	62	0,54	78	0,53	94	0,46	110	0,51	126	0,45
15	0,53	31	0,47	47	0,53	63	0,45	79	0,46	95	0,53	111	0,42	127	0,44
16	0,5	32	0,45	48	0,38	64	0,55	80	0,56	96	0,55	112	0,46	128	0,5

Сурет 6 – Биттік шашырау критерийінің бит орындарына сәйкес өзгеру ықтималдығы

бульдік функцияларға негізделген S-блоктардың құрылымы жайлы ең алғаш Адамс пен С. Таварес, Квангжо Ким еңбектерінде зерттелді. Бульдік функцияның қатаң лавиндік критерийін зерттеу келесі белгілеулер, ұғымдар мен анықтамаларға негізделген [18].

Бізде F_2^n – n өлшемді екілік векторлық кеңістік болсын және мұндағы $F_2 - \{0,1\}$ элементтерінен тұратын Галуа өрісі болсын. n және m - натурал сандар болсын, онда векторлы бульдік функция F-ті мына түрде анықтаймыз: $F : F_2^n \mapsto F_2^m$.

1-анықтама. $F(x) = (f_1, f_2, \ldots, f_m)$ функциясындағы $f_1, f_2, \ldots, f_m$ – бульдік функциялары F бульдік функцияның координаталары деп аталады. $m = 1$ кезінде векторлы бульдік функция шығысында тек бір бит ғана болатын кәдімгі бульдік функцияға эквивалентті.

2-анықтама. $f(x) : F_2^n \mapsto F_2$ – n айнымалысы бар бульдік функция болсын, мұндағы $x = (x_0, x_1, \ldots, x_{n-1})$. Онда $f(x)$ функциясының хемминг салмағы былай анықталады:

$$hw(f) = \sum_{x=0}^{2^n-1} f(x). \tag{4}$$

3-анықтама. $f(x): F_2^n \mapsto F_2$ бульді функциясы болсын. Онда $f(x)$ функциясының $u \in F_2^n$ екілік векторы арқылы алынған өсімшесі былай анықталады:

$$D_u f(x) = f(x) \oplus f(x+u). \tag{5}$$

4-анықтама. Қандай да бір бульдік функция $f(x)$ қатаң лавиндік критерийді қанағаттандырады деп айтамыз, егер $u \in F_2^n$ үшін төмендегідей теңдеулер жүйесі орындалса:

$$\begin{cases} hw(u) = 1; \\ \sum_{x=0}^{2^n-1} (f(x) \oplus f(x+u)) = 2^{n-1}. \end{cases} \tag{6}$$

немесе ықтималдықтар түрінде былай жазуға болады:

$$\begin{cases} hw(u) = 1; \\ p\{f(x) = f(x+u)\} = 0.5. \end{cases} \tag{7}$$

Енді, негізгі жұмыс — S-блоктарға қатаң лавиндік критерийді тексеруге көшейік. Түсінікті болу үшін төрт "алтын" S-блоктың біріншісіне (S_1 -блок) жүргізілген талдауды толықтай қадамдап жүргізейік. S_1 -блокты декомпозиция арқылы бульдік функция компоненттерімен жазып алайық:

Кесте 3 – S_1 **-дің компоненттік жазбасы**

$S_1 =$	0	F	B	8	C	9	6	3	D	1	2	4	A	7	5	E
1-жол	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0
2-жол	0	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1
3-жол	0	1	0	0	1	0	1	0	1	0	0	1	0	1	1	1
4-жол	0	1	1	1	1	1	0	0	1	0	0	0	1	0	0	1

Бұдан әрі, Кесте-3-тен біз S-box бірінші жолдың компоненттік мәндері негізінде төрт айнымалысы бар $(n = 4)$ бульдік функциясын қатаң лавиндік критерийіне сәйкестігін зерттеуге көшеміз:

$$f_1(x_1, x_2, x_3, x_4) = \{0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0\}. \tag{8}$$

Бұдан әрі 3-ші және 4-анықтамаға сүйене отырып, келесі кестені құрайық. Бұл Кесте-4-те $f_1(x)$ бульдік функцияның төрт айнымалысының барлық мүмкін мәндеріндегі (8)-өрнекке сәйкес нәтижелері, $f_1(x)$ бульдік функцияның $hw(u) = 1$ өсімшесімен қосылған аргументіндегі мәні және $D_u f_1(x)$ (Кестеде D_u деп белгіленген) өсімшесінің нәтижелері көрсетілген.

Енді, Кесте-3-ті пайдаланып, осындай есептеулерді біз S_1 -блоктың 2-ші, 3-ші және 4-ші жолдарының компоненттік мәндері:

$$\begin{gathered} f_2(x_1, x_2, x_3, x_4) = \{0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1\}, \\ f_3(x_1, x_2, x_3, x_4) = \{0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1\}, \\ f_4(x_1, x_2, x_3, x_4) = \{0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1\} \end{gathered}$$

үшін жүргіземіз. Соңында, S_1 -блоктың барлық жолдарының компоненттері арқылы алынған нәтижелер төмендегідей матрица түрінде өрнектейік:

$$SAC_{S_1} = \begin{pmatrix} \Sigma D_{0001} f_1(x) & \Sigma D_{0010} f_1(x) & \Sigma D_{0100} f_1(x) & \Sigma D_{1000} f_1(x) \\ \Sigma D_{0001} f_2(x) & \Sigma D_{0010} f_2(x) & \Sigma D_{0100} f_2(x) & \Sigma D_{1000} f_2(x) \\ \Sigma D_{0001} f_3(x) & \Sigma D_{0010} f_3(x) & \Sigma D_{0100} f_3(x) & \Sigma D_{1000} f_3(x) \\ \Sigma D_{0001} f_4(x) & \Sigma D_{0010} f_4(x) & \Sigma D_{0100} f_4(x) & \Sigma D_{1000} f_4(x) \end{pmatrix} = \begin{pmatrix} 12 & 12 & 8 & 8 \\ 8 & 12 & 12 & 8 \\ 12 & 8 & 12 & 12 \\ 8 & 12 & 8 & 12 \end{pmatrix}. \tag{9}$$

Кесте 4 – берілген $f(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_1(x)$	$f_1(x \oplus 0001)$	D_{0001}	$f_1(x \oplus 0010)$	D_{0010}	$f_1(x \oplus 0100)$	D_{0100}	$f_1(x \oplus 1000)$	D_{1000}
$f(0000)=0$	$f(0001)=1$	1	$f(0010)=1$	1	$f(0100)=0$	0	$f(1000)=1$	1
$f(0001)=1$	$f(0000)=0$	1	$f(0011)=0$	1	$f(0101)=1$	0	$f(1001)=1$	0
$f(0010)=1$	$f(0011)=0$	1	$f(0000)=0$	1	$f(0110)=0$	1	$f(1010)=0$	1
$f(0011)=0$	$f(0010)=1$	1	$f(0001)=1$	1	$f(0111)=1$	1	$f(1011)=0$	0
$f(0100)=0$	$f(0101)=1$	1	$f(0110)=0$	0	$f(0000)=0$	0	$f(1100)=0$	0
$f(0101)=1$	$f(0100)=0$	1	$f(0111)=1$	0	$f(0001)=1$	0	$f(1101)=1$	0
$f(0110)=0$	$f(0111)=1$	1	$f(0100)=0$	0	$f(0010)=1$	1	$f(1110)=1$	1
$f(0111)=1$	$f(0110)=0$	1	$f(0101)=1$	0	$f(0011)=0$	1	$f(1111)=0$	1
$f(1000)=1$	$f(1001)=1$	0	$f(1010)=0$	1	$f(1100)=0$	1	$f(0000)=0$	1
$f(1001)=1$	$f(1000)=1$	0	$f(1011)=0$	1	$f(1101)=1$	0	$f(0001)=1$	0
$f(1010)=0$	$f(1011)=0$	0	$f(1000)=1$	1	$f(1110)=1$	1	$f(0010)=1$	1
$f(1011)=0$	$f(1010)=0$	0	$f(1001)=1$	1	$f(1111)=0$	0	$f(0011)=0$	0
$f(1100)=0$	$f(1101)=1$	1	$f(1110)=1$	1	$f(1000)=1$	1	$f(0100)=0$	0
$f(1101)=1$	$f(1100)=0$	1	$f(1111)=0$	1	$f(1001)=1$	0	$f(0101)=1$	0
$f(1110)=1$	$f(1111)=0$	1	$f(1100)=0$	1	$f(1010)=0$	1	$f(0110)=0$	1
$f(1111)=0$	$f(1110)=1$	1	$f(1101)=1$	1	$f(1011)=0$	0	$f(0111)=1$	1
		Σ=12		Σ=12		Σ=8		$\Sigma=8$

Дәл осындай есептеу жолымен біз қолданған S_2-блок, S_3-блок және S_4-блок үшін төмендегідей нәтижелер аламыз:

$$SAC_{S_2}=\begin{pmatrix}8&12&12&8\\12&8&12&8\\12&8&12&8\\12&12&8&12\end{pmatrix}, SAC_{S_3}=\begin{pmatrix}12&8&12&8\\8&12&12&8\\8&12&12&8\\12&8&8&12\end{pmatrix}, SAC_{S_4}=\begin{pmatrix}12&12&8&8\\12&8&8&12\\8&12&12&12\\8&12&8&12\end{pmatrix}. \tag{10}$$

(6)-формулаға сүйенсек, алынған мәндер оң нәтиже беру үшін олар $N/2=8$ саны маңында болуы тиіс, мұндағы $N=2^4$. (9) бен (10)-нан байқайтынымыз, таңдап алынған S-блок алмастырулар қатаң лавиндік эффектіні (SAC) орта есеппен 70-75% қанағаттандырады, яғни оларды шифрлау алгоритмінің тиімді примитиві ретінде қолдануға болады. Дегенмен, тәжірибеде SAC-ті 100% қанағаттандыратын кейбір S-блоктар дифференциалдық талдауға төзімсіздік танытып жатады: мысалы дереккөз [17]-де қарастырылған S-блок – $S=\{4,7,2,14,1,13,8,11,15,12,6,10,5,9,3,0\}$. Сол себепті, алдағы уақытта қарастырып отырған S-блоктарға дифференциалды және сызықты талдау, олардың векторлық бульдік функциялар арқылы жазбасындағы сызықсыздық дәрежесін, қасиеттерін және коррелациялық, алгебралық, статистикалық талдаулар негізіндегі шабуылдарға төзімділігін анықтау бағытында зерттеулер жүргізу қажеттілігі туындады.

2.3.3. CF шифрлау алгоритмінің қатаң лавиндік эффектін зерттеу

Шифрлау алгоритмінің қатаң лавиндік критерийі

$$\varepsilon_s=|2*k_{si,j}-1| \tag{11}$$

арқылы бағаланады, мұндағы i – шифрлаудың кіріс мәндегі өзгертілген биттің нөмірі, j – шифрлаудың шығыс мәніндегі талданатын биттің нөмірі, $k_{si,j}$ – j–ші шығыс биттің өзгертілген i-ші кіріс битке қатысты өзгеруінің ықтималдығы. Яғни, бұл критерий лавиндік критерийге қарағанда талапты жоғары қояды: өзгертілген әрбір кіріс битіне байланысты әрбір шығыс битінің өзгеру қасиетін қарастырады. Теорияда бұл өзгерістің ықтималдығы 0,5-ке жуықтау болуы қажет.

Тәжірибеде талдауымызды мына бағытта жүргіземіз. Алдымен P_0^k ашық мәтінді толық 4 раундпен шифрлаймыз, нәтижені C_0^k деп белгілейік, мұндағы k – ашық мәтіндер нөмірі. Талдау үшін ашық мәтіннің әрбір кіріс i–битін инверсиялап, оны P_i^k ретінде

қарастырып, шифрлау арқылы соған сәйкес C_i^k шифрмәтінін алып отырамыз, мұнда $i = 1, \ldots, 128$. Әрбір P_i^k үшін C_i^k шифрмәтіндегі j–ші битті бастапқы C_0^k шифрмәтіндегі j–ші битімен салыстыратын боламыз, мұндағы $j = 1, \ldots, 128$. Бізге салыстыру нәтижелеріне талдау жүргізу үшін төмендегідей 128x128 өлшемдегі Q^k матрицасы қажет болады:

$$Q^k = \begin{pmatrix} q_{1,1}^k & q_{1,2}^k & \cdots & q_{1,128}^k \\ q_{2,1}^k & q_{2,2}^k & \cdots & q_{2,128}^k \\ \cdots & \cdots & \cdots & \cdots \\ q_{128,1}^k & q_{128,2}^k & \cdots & q_{128,128}^k \end{pmatrix}. \tag{12}$$

Мұнда, $q_{i,j}^k$ – P_0^k ашық мәтіннің i–битін инверсиялап, шифрлау жүргізгенде алынған C_i^k шифрмәтіннің j–ші битінің C_0^k шифрмәтіндегі j–ші битімен салыстыратын өзгеруі, яғни

$$q_{i,j}^k = \begin{cases} 1, & \text{салыстыруда өзгеріс болса;} \\ 0, & \text{салыстыруда өзгеріс болмаса.} \end{cases} \tag{13}$$

Қатаң лавиндік критерийдің орындалуын эмипирикалық түрде тексеру үшін біз әртүрлі екі жүз P_0^k ашық мәтін алдық, $k = 1, 2, \ldots, 200$. Әр k үшін жоғарғы процесті жүргізіп, сәйкесінше екі жүз Q^k алатын боламыз. Алынған екі жүз Q^k матрицасының k бойынша сәйкес элементтерінің қосындысын шығарып, оны төмендегідей белгілейік:

$$R = \begin{pmatrix} \sum_{k=1}^{200} q_{1,1}^k & \sum_{k=1}^{200} q_{1,2}^k & \cdots & \sum_{k=1}^{200} q_{1,128}^k \\ \sum_{k=1}^{200} q_{1,1}^k & \sum_{k=1}^{200} q_{1,2}^k & \cdots & \sum_{k=1}^{200} q_{1,128}^k \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{k=1}^{200} q_{128,1}^k & \sum_{k=1}^{200} q_{128,2}^k & \cdots & \sum_{k=1}^{200} q_{128,128}^k \end{pmatrix}. \tag{14}$$

Бұдан әрі, $p_{si,j}$ ықтималдығын алу үшін R матрицасының әр элементін ашық мәтіндер санына - 200-ге бөлеміз, сонда:

$$Pr_s = \begin{pmatrix} p_{s1,1} & p_{s1,2} & \cdots & p_{s1,128} \\ p_{s2,1} & p_{s2,2} & \cdots & p_{s2,128} \\ \cdots & \cdots & \cdots & \cdots \\ p_{s128,1} & p_{s128,2} & \cdots & p_{s128,128} \end{pmatrix}. \tag{15}$$

Алынған $p_{si,j}$ негізінде (11) формула арқылы CF шифрлау алгоритмінің қатаң лавиндік критерийін қанағаттандыруын бағалайтын боламыз, мұндағы $i, j = 1, \ldots, 128$. Бұл есептеулерді жүргізу үшін "Ақпараттық қауіпсіздік" зертханасында арнайы компьютерлік бағдарлама әзірленді. Бағдарлама көмегімен таңдап алынған 200 ашық мәтінге қатаң лавиндік критерийін анықтау мақсатында төмендегідей ықтималдықтар матрицасын алдық:

$$Pr_s = \begin{pmatrix} 0,56 & 0,50 & 0,51 & 0,54 & 0,53 & 0,46 & ... & 0,53 \\ 0,52 & 0,50 & 0,50 & 0,49 & 0,49 & 0,47 & ... & 0,47 \\ 0,49 & 0,41 & 0,42 & 0,47 & 0,53 & 0,51 & ... & 0,57 \\ 0,47 & \mathbf{0,45} & 0,44 & 0,52 & 0,50 & 0,55 & ... & 0,51 \\ 0,49 & 0,51 & 0,49 & 0,47 & 0,51 & 0,45 & ... & 0,53 \\ 0,55 & 0,59 & 0,47 & 0,48 & 0,51 & 0,49 & ... & 0,53 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0,45 & 0,56 & 0,54 & 0,47 & 0,51 & 0,61 & ... & 0,51 \end{pmatrix}. \tag{16}$$

Мысалы, 200 ашық мәтіннің әрбір 4–ші битін инвертациялап шифрлағанда, 200 шифрмәтіннің әрқайсының 2–ші битінің бастапқы инвертацияланбаған нұсқасынан өзгеру ықтималдығы тәжірибе жүзінде 0,45–ке тең болды.

(11) формула көмегімен төмендегі 5–кестеде көрсетілген ε_s қатаң лавиндік параметрдің статистикалық көрсеткіштерін алдық.

CF шифрлау алгоритмінің қатаң лавиндік критерийін талдауы бойынша қорыта келгенде, 5-кестедегі мәндер теориялық тұрғыдан алғанда оң нәтижелер көрсетеді. Осы нәтижелер көрсеткендей, шифрлаудың кірісіндегі әрбір i–ші биттің өзгерісі шифрмәтіннің

Кесте 5 – ε_s **қатаң лавиндік параметрдің статистикалық көрсеткіштері**

	Pr_s ықтималдығы	ε_s–нің мәндері
Максимальды мән	0,6562	0,3125
Минималді мән	0,3437	0
Арифметикалық орта мән	0,5004	0,0710
Дисперсия	0,0018	0,0027
Мода	0,5078	0,0156
Медиана	0,5000	0,0625

j –ші битінің өзгерісін 0,5 ықтималдықтен туындатады. Осы себепті аталған алгоритм қатаң лавиндік критерийін толық қанағаттандырады.

2.3.4. Шифрлау алгоритмінің тиімді раундтар санын анықтау

Қарастырылған шифрлау алгоритміне жүргізілген лавиндік және қатаң лавиндік критерийлердің сараптамаларын бағалау нәтижесінде бойынша раундтар санының төменгі мәні 4 ретінде қарастыру жеткілікті. Раунд санының ең тиімді мәнін таңдап алу мақсатында төмендегідей фактілерді ескерген жөн.

Алгоритм жұмыс істеу сұлбасында көрсетілгендей, бір раунд ішінде S-блок алмастыруы екі рет жүргізіледі, яғни Stage-1 және Stage-3 түрлендіруінде. Айта кететін жайт, осы екі түрлендірулерде сызықты (xor) және сызықты емес операциялар әр байтты есептеу барысында кезектесіп орындалып отырады. Бұл өз кезегінде диффузиялық қасиеттің жоғарғы деңгейге жетуіне әкеледі. Оның дәлелі ретінде 1-раундтан кейінгі биттік шашырау нәтижесінен көруге болады.

Төменгі Кесте-6–да ε_α лавиндік параметрінің 1, 2, 4, 8, 12–раундтардан кейінгі статистикалық көрсеткіштері көрсетілген. Осы кестеден байқайтынымыз, 1–ші және 2–раундтарда статистикалық көрсеткіштер қалған раундтар көрсеткіштеріне қарағанда нашарлау, ал 4–раундтан бастап әрі қарай раунд ұлғайған сайын да мәндер бір-бірлерімен шамалас болып отыр.

Алынған лавиндік эффект нәтижелерінің қорытындысы бойынша раундтар саны әзірше 4–ке тең болуы жеткілікті болды. Алайда, дифференциалды, сызықты, алгебралық және де басқа заманауи криптоталдау әдістеріне төтеп беру үшін, сондай-ақ кілттердің әрбір биті шифрмәтіннің әрбір битіне әсер ету мәселесі, шығатын биттердің бір-біріне тәуелсіздік мәселесі сияқты тағы да басқа маңызды мәселелер раунд санының артуына алып келуі мүмкін, осы бағытта алдағы уақытта зерттеулер жүргізу талап етіледі.

Кесте 6 – ε_α **лавиндік параметрдің статистикалық көрсеткіштері**

ε_α статистикалық көрсеткіштері	1–раунд	2–раунд	**4–раунд**	8–раунд	12–раунд
Максимальды мән	0,2814	0,3437	**0,2400**	0,2342	0,2343
Минималді мән	0	0	**0**	0	0
Арифметикалық орта мән	0,0743	0,0711	**0,0668**	0,0702	0,0713
Дисперсия	0,0026	0,0037	**0,0022**	0,0029	0,0029
Мода	0,0625	0	**0,0460**	0	0,0468
Медиана	0,0625	0,047	**0,0500**	0,0425	0,0625

2.3.5. CFKey раундтық кілттерді жасау алгоритмін талдау

Қарастырылған CFKey алгоритмінде бастапқы құпия кілт арқылы бізге қажетті жасалынатын төрт раундтық кілттердің қауіпсіздік дәрежесін анықтайық. Осы мақсатта бастапқы кілттің әрбір битінің өзгерісі CF шифрлау алгоритмі арқылы алынған шифрмәтінді қаншалықты деңгейде өзгеріске ұшырататыны бағытында зерттеу жұмысы жүргізілді. Басқа сөзбен айтқанда, шифрмәтіннің бастапқы кілтке қатысты "лавиндік эффекті" тексерілді. Ол үшін 128 биттік ұзындықтағы бастапқы кілт ретінде

0xCC156C4CE0024D5113D680D7CCE6D8B2 кездейсоқ таңдап алдық. Осы кілттің әрбір битін кезектеп инверсиялап, қосымша 128 бастапқы кілт алдық. Әрі қарай, 129 кілт арқылы кездейсоқ таңдалған "Alga_Kazakhstan!" ашық мәтінін шифрлап, сәйкес 129 шифрмәтін алдық. Осылайша, нәтижелерді талдап, CFKey алгоритмі арқылы жасалған раундтық кілттердің "лавиндік критерийді" қанағаттандыратынына көз жеткізейік.Сурет-7-ден әрбір 1-ден 128-ге дейінгі жеке-жеке өзгерген биттер үшін шифрмәтіннің жалпы мәндерінің өзгеру ықтималдығын көруге болады. Кесте-7-де арнайы бағдарлама

Кесте 7 – Кілттің ε_α лавиндік параметрге әсері

i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α	i	ε_α
1	0,05	17	0,16	33	0,03	49	0,14	65	0,11	81	0,05	97	0,02	113	0,14
2	0,13	18	0,03	34	0,05	50	0,03	66	0,03	82	0,17	98	0,09	114	0,08
3	0,02	19	0,11	35	0,09	51	0,08	67	0,02	83	0,16	99	0,03	115	0,06
4	0,02	20	0,13	36	0,02	52	0,00	68	0,09	84	0,06	100	0,05	116	0,13
5	0,03	21	0,06	37	0,08	53	0,03	69	0,03	85	0,22	101	0,03	117	0,11
6	0,08	22	0,09	38	0,11	54	0,05	70	0,13	86	0,02	102	0,00	118	0,11
7	0,05	23	0,03	39	0,05	55	0,14	71	0,02	87	0,03	103	0,02	119	0,03
8	0,09	24	0,03	40	0,19	56	0,00	72	0,03	88	0,05	104	0,14	120	0,06
9	0,08	25	0,02	41	0,09	57	0,03	73	0,09	89	0,03	105	0,06	121	0,06
10	0,09	26	0,13	42	0,08	58	0,11	74	0,03	90	0,05	106	0,03	122	0,02
11	0,05	27	0,08	43	0,02	59	0,02	75	0,03	91	0,11	107	0,02	123	0,00
12	0,02	28	0,16	44	0,05	60	0,00	76	0,19	92	0,00	108	0,05	124	0,03
13	0,03	29	0,13	45	0,02	61	0,11	77	0,06	93	0,09	109	0,11	125	0,22
14	0,11	30	0,05	46	0,06	62	0,05	78	0,05	94	0,09	110	0,17	126	0,02
15	0,02	31	0,13	47	0,02	63	0,02	79	0,05	95	0,11	111	0,09	127	0,02
16	0,20	32	0,02	48	0,13	64	0,11	80	0,11	96	0,23	112	0,16	128	0,11

арқылы алынған 128 шифрмәтіннің ε_α лавиндік әсері параметрінің әрбір өзгерген бит орындарындағы мәндері, ал кесте-8-де осы мәндердің статистикалық көрсеткіштері көрсетілген.

Кесте 8 – ε_α лавиндік параметрдің статистикалық көрсеткіштері

Минималді мән	Максимальды мән	Арифметикалық орта мән	Дисперсия
0	0,23	0,07	0,002

Сурет 7 – Биттік шашырау критерийінің бит орындарына сәйкес өзгеру ықтималдығы

Кесте-7 мен Кесте-8 және Сурет-7-ден мынандай қортынды шығаруға болады:

кездейсоқ алынған бастапқы құпия кілттен алынатын раундтық кілттердің негізінде алынған шифрмәтін осы бастапқы кілттің әрбір битінің өзгерісіне 0,5 ықтималдықтен тәуелді. Яғни, бастапқы кілттің өте аз өзгерісі шифрмәтіннің биттерін 50 пайыздық өзгеріске ұшыратады. Бұл қасиет CFKey алгоритмі раундтық кілттерге қойылатын талаптарға сай екендігін көрсетеді. CF алгоритміндегі мынандай ерекшелік бар: оның құрамындағы SBOX процедурасы арқылы бірдей мәндерден тұратын ашық мәтін мәндердің орналасу орнына байланысты белгілі тәртіппен S-блоктан өткенде, әртүрлі шығыс мәтіндер беретін болады. Мысалы, 16 байттан тұратын құпия кілт былай алынсын: $(32, 32, 32, 32, \ldots, 32)_{16}$, сонда келесідегідей бір-бірінен өзгеше шығыс мәндер аламыз:

$$A = \begin{pmatrix} 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 \end{pmatrix} \overset{SBOX}{\rightarrow} \begin{pmatrix} B8 & E8 & F8 & 38 \\ B1 & E1 & F1 & 31 \\ B5 & E5 & F5 & 35 \\ B4 & E4 & F4 & 34 \end{pmatrix}. \tag{17}$$

Бұның сыртында StageKey-1 және StageKey-3 түрлендірулерінде матрицаның әр элементін есептегенде, xor операциясы мен S-блоктан өткізу операциясы кезектесіп орындалатынын есепке алатын болсақ, "осал кілттер" классы тарыла түседі.

3. Қорытынды

Бұл мақалада блоктық шифлау алгоритмдерінің негізгі талаптары мен ұсыныстарын қанағаттандыратын жаңа CF симметриялық блокты шифрлау алгоритмі құрылымы, оның кілт жасау алгоритмі, бағдарламалық жүзеге асырылуы және "лавиндік эффект" қасиеті мен "қатаң лавиндік эффект" қасиеті көрсетілген. Алгоритмнің құрамындағы сызықты және сызықты емес түрлендіру әдістеріне жеке-жеке тоқталып, алгоритмнің жұмыс құрылымы түсіндірілді. Сонымен бірге, жұмыс істеу өнімділігі талданып, оның жылдамдығы жағынан жақсы көрсеткіш көрсеткені анықталған, яғни бағдарлама көмегімен әр түрлі өлшемдегі, кеңейтуі әртүрлі файлдарды алып шифрлап, шифрлау жылдамдығы жылдам жасайтындығы анықталды. Алгоритмның биттік шашырату критерийі 1-ші раундтан кейін-ақ қажетті деңгейде екені көрсетілді. CF шифрлау алгоритмінің қатаң лавиндік критерийін талдауы қорытындысы бойынша да оң нәтижелер алынды. Жұмыс барысында қолданылатын төрт S-блоктардың қатаң лавиндік критерийін қанағаттандыруы тексерілді. Алайда, қажетті мөлшердегі раунд саны әзірше – 4, ол алдағы уақытта криптоберіктілікті талдау барысында жұмыс өнімділігін ескере отырып, әлі де нақтыланатын болады. Қазіргі уақытта алгоритмнің криптоберіктілігін статистикалық және алгебралық тәсілдермен талдау жұмыстары жүргізуде.

4. Алғыс

Жұмыс OR11465439 "Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хэштеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау" бағдарламалық-нысаналық қаржыландыру ғылыми жобасы аясында жүргізілді.

Әдебиеттер тізімі

1 Столлингс В. Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. - Москва: Вильямс, 2001. -672 с.

2 Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - Москва: Гелиос АРВ, 2006. - 376 с.

3 Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Конечные поля. - Москва: КУДИЦ-ОБРАЗ, 2002. - 176 с.

4 Панасенко С.П. Алгоритмы шифрования. Специальный справочник. -СПб.: БХВ-Петербург, 2009. - 576 с.

5 Д.С. Дюсенбаев, К.Т. Алғазы, Қ.С. Сақан. Симметриялы шифрларда қолданылатын сызықты емес түйіндерді зерттеу // Матер. межд. науч.-практ. конф. "Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020". - Алматы, 2020. - Б.34-39.

6 Aboushosha B., Ramadan R.A., Dwivedi A.D., El-Sayed A. and Dessouky M.M. SLIM: "A Lightweight Block Cipher for Internet of Health Things", in IEEE Access. -2020. -Vol. 8. -P. 203747-203757. -doi: 10.1109/ACCESS.2020.3036589. (01.09.2021).
7 Ghosha A., Sadhukhan R., Patranabis S., Datta N., Picek S., Mukhopadhyay D. Lightweight and Side-channel Secure 4x4 S-Boxes from Cellular Automata Rules// IACR Transactions on Symmetric Cryptology. -2018. 3. P. 311-334. https://doi.org/10.13154/tosc.v2018.i3.311-334. (21.08.2021).
8 Hicks C., Garcia F. D., Oswald D. Dismantling the AUT64 Automotive Cipher// IACR Transactions on Cryptographic Hardware and Embedded Systems. -2018(2). -P. 46-69. URL: https://doi.org/10.13154/tches.v2018.i2.46-69. (02.10.2021).
9 Jiqiang Lu, Hwajung Seo A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design// Security and Communication Networks. -2020. Vol. 2020. 1-26 pages, URL: https://doi.org/10.1155/2020/1457419. (21.07.2021).
10 Горбенко И.Д., Долгов И.В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И. Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования // Известия ЮФУ. Технические науки. -2007. №1. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.03.2021).
11 Saarinen, Markku-Juhani O. Cryptographic Analysis of All 4 x 4 - Bit S-Boxes// Selected Areas in Cryptography. SAC 2011. Lecture Notes in Computer Science. -2012. -vol 7118. pp. 118-133, Springer, Berlin, Heidelberg. $https://doi.org/10.1007/978-3-642-28496-0_7$
12 Anderson R., Biham E. and Knudsen L. Serpent: A Proposal for the Advanced Encryption Standard// NIST AES Proposal, 1998, pp. 1-23. Available at: http://www.cl.cam.ac.uk/ rja14/Papers/serpent.pdf (1999) (14.09.2021).
13 Engels D., Fan X., Gong G., Hu H. and Smith E. M. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices// In R. Sion et al. (Eds.): FC 2010 Workshops, LNCS 6054, -P. 3-18. Springer.
14 Engels D., Saarinen M.-J. O., Schweitzer P. and Smith E. M. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm//RFIDSec 2011, The 7th Workshop on RFID Security and Privacy, 26-28 June 2011, Amherst, Massachusetts, USA (2011).
15 Vergili I., Y?cel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen? S-Boxes // Turk J Elec Engin. - 2001. - T. 9, № 2. - P. 137-145.
16 Levinskas Matas, Mihalkovich Aleksejus Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power// Mathematical Models in Engineering. -2021. -Vol. 7. -Issue 3. -P. 50-53. URL: https://doi.org/10.21595/mme.2021.22234. (10.08.2021).
17 Сейткулов, Е., Оспанов, Р., Ергалиева, Б. On cryptographic properties of S-boxes// VESTNIK KAZNRTU. -2021. -Vol. 143. No 4. -P. 96-103. URL: https://doi.org/10.51301/vest.su.2021.i4.12.
18 Sokolov A., Zhdanov O. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength// Siberian Journal of Science and Technology. -2019. 20. -P. 183-190.

С.Е.Нысанбаева [1,2] , К.Т. Алгазы [1] , Қ.С.Сакан [1,2] , А.Хомпыш [1,2] , Д.С.Дуйсенбаев [1]

[1] *Институт информационных и вычислительных технологий, г. Алматы, Казахстан*
[2] *Казахский национальный университет им. аль-Фараби, г.Алматы, Казахстан*

Блочный алгоритм шифрования CF и исследование его критерий лавинного эффекта

Аннотация: В статье описываются значимость, особенность и область применения симметричных блочных шифров, используемых для обеспечения конфиденциальности данных в процессе развития современных вычислительных технологий. Кратко изложена структура алгоритма шифрования "CF" и механизм генерации раундовых ключей на основе основного ключа симметричного блока, разработанного в Лаборатории информационной безопасности Института информационных и вычислительных технологий. Разработана программная реализация созданного алгоритма шифрования, на основе которого проверены производительность работы и битовое рассеивание (свойство "лавинного эффекта" и свойство "строгого лавинного эффекта") между открытым текстом и соответствующим ему шифртекстом. С целью оптимизации аппаратной реализации алгоритма применено преобразование S-блока замены, рассматриваемое как нелинейный узел, размером 4x4 бит.

Ключевые слова: алгоритмы шифрования, криптостойкость алгоритма, критерий "лавинного эффекта", критерий "строгого лавинного эффекта".

S.E.Nyssanbayeva [1,2] , K.Algazy [1] , K.S.Sakan [1,2] , A. Khompysh [1,2] , D.S.Dyussenbayev [1]

[1] *Institute of Information and Computing Technologies, Almaty, Kazakhstan*
[2] *al-Farabi Kazakh National University, Almaty, Kazakhstan*

The encryption algorithm "FC" and analysis of its avalanche effect criterion

Abstract: The article is about the importance, features and scope of symmetric block ciphers used to ensure the confidentiality of data in the era of rapid development of modern computing technologies. In this paper, the structure of the symmetric block encryption algorithm CF, developed in the "Laboratory of Information Security" of the "Institute of Information and Computational Technologies", the round keys generating mechanism based on it's secret key are described.

A computer program of the created encryption algorithm was developed, on the basis of which the performance was studied and the bit scattering between the plaintext and the ciphertext (the property of the "avalanche effect" and "strong avalanche effect") was checked. In order to optimize the hardware implementation of the algorithm, the conversion of the S-block, which is considered as a nonlinear node, was obtained in 4x4 bit size.

Keywords: encryption algorithm, cryptographic strength, avalanche effect, strong avalanche effect.

References

1 Stalling W. Kriptografiya i zashchita setej: principy i praktika [Cryptography and Network Security: Principles and Practice]. Second Edition. Trans. from eng. (Williams, Moscow, 2001, 672 p.).

2 Babenko L.K., Ishchukova E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ih analiza [Modern block encryption algorithms and methods of their analysis]. (Helios, Moscow, 2006. 376 p.).

3 Zenzin O.S., Ivanov M.A. Standart kriptograficheskoj zashchity - AES [AES - Cryptographic Security Standard]. Finite field. (KUDITS-OBRAZ, Moscow, 2002. 176 p.).

4 Panasenko S.P. Algoritmy shifrovaniya. Special'nyj spravochnik. [Encryption algorithms. A special reference book] (bhv, Saint Petersburg, 2009, 576 p.).

5 Dyusenbaev D.S., Algazy K.T., Sakan K.S. Simmetriyalyi shifrlarda koldanyilatyin sizyiktyi emes tuinderdi zertteu [Study of nonlinear nodes used in symmetric ciphers], Mater. of Int. Sci.-pract. Conf. " Actual problems of information security in Kazakhstan APIBK-2020". Almaty, 2020. 34-39.

6 Aboushosha B., Ramadan R.A., Dwivedi A.D., El-Sayed A. and Dessouky M. M. SLIM: A Lightweight Block Cipher for Internet of Health Things, in IEEE Access. Vol. 8, P. 203747-203757, 2020, doi: 10.1109/ACCESS.2020.3036589. (01.09.2021).

7 Ghoshal A., Sadhukhan R., Patranabis S., Datta N., Picek S., Mukhopadhyay D. Lightweight and Side-channel Secure 4x4 S-Boxes from Cellular Automata Rules. IACR Transactions on Symmetric Cryptology, 2018(3), 311-334. https://doi.org/10.13154/tosc.v2018.i3.311-334. (21.08.2021).

8 Hicks C., Garcia F.D., Oswald D. Dismantling the AUT64 Automotive Cipher. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(2), 46-69. Available at: https://doi.org/10.13154/tches.v2018.i2.46-69. (02.10.2021).

9 Jiqiang Lu, Hwajung Seo A Key Selected S-Box Mechanism and Its Investigation in Modern Block Cipher Design, Security and Communication Networks, 2020, Vol. 2020, 1-26 pages, 2020. Available at: https://doi.org/10.1155/2020/1457419. (21.07.2021).

10 Gorbenko I.D., Dolgov I.V., Oleynikov R.V., Rujentsev V.I., Mihaylenko M.S., Gorbenko YU.I. Razrabotka trebovaniy i printsip proektirovaniya perspektivnogo simmetrichnogo blochnogo algoritma shifrovaniya [Development of requirements and the design principle of a promising symmetric block encryption algorithm]// Izvestiya SFedU. Engineering sciences. 2007. №1. Available at: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.03.2021).

11 Saarinen, Markku-Juhani O. Cryptographic Analysis of All 4 x 4 - Bit S-Boxes, Selected Areas in Cryptography. SAC 2011. Lecture Notes in Computer Science, vol 7118, 2012, pp. 118-133, Springer, Berlin, Heidelberg. $https://doi.org/10.1007/978-3-642-28496-0_7$

12 Anderson R. , Biham E. and Knudsen L. Serpent: A Proposal for the Advanced Encryption Standard, NIST AES Proposal, 1998, pp. 1-23. Available at: http://www.cl.cam.ac.uk/ rja14/Papers/serpent.pdf (1999) (14.09.2021).

13 Engels D., Fan X., Gong G., Hu H. and Smith E.M. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices, In R. Sion et al. (Eds.): FC 2010 Workshops, LNCS 6054, pp. 3-18. Springer.

14 Engels D., Saarinen M.-J. O., Schweitzer P., and Smith E. M. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm, RFIDSec 2011, The 7th Workshop on RFID Security and Privacy, 26-28 June 2011, Amherst, Massachusetts, USA (2011).

15 Vergili I., Y?cel M. D. Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen? S-Boxes, Turk J Elec Engin, 9(2), 137-145(2001).

16 Levinskas Matas, Mihalkovich Aleksejus Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power, Mathematical Models in Engineering, 7(3), 50-53(2021). Available at: https://doi.org/10.21595/mme.2021.22234. (10.08.2021).

17 Seitkulov Y.N., Ospanov R.M., Yergaliyeva B.B. On cryptographic properties of S-boxes, VESTNIK KAZNRTU, 143(4), 96-103(2021). Available at: https://doi.org/10.51301/vest.su.2021.i4.12.

18 Sokolov A., Zhdanov O. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength, Siberian Journal of Science and Technology. 20. 183-190(2019). 10.31772/2587-6066-2019-20-2-183-190.

Авторлар туралы мағлұмат:

Нысанбаева С.Е. – т.ғ.д., қауымд. профессор, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының бас ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Алгазы К.Т. – Phd, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Сақан К.С – ***корреспонденция үшін автор***, әл-Фараби атындағы ҚазҰУ Phd докторанты, әл-Фараби даңғылы, 71 үй, 050040, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Хомпыш А. – PhD, ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Дүйсенбаев Д.С. – ҚР БҒМ ҒК АЕТИ ақпараттық қауіпсіздік зертханасының ғылыми қызметкері, Шевченко к-сі, 28 үй, 050010, Алматы қ., Қазақстан.

Nyssanbayeva S.E. – Dr.Tech.Sc., sassociate professor, Chief researcher of Information security laboratories, IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Algazy K.T. – PhD, researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Sakan K.S – ***correspondence author***, Phd student KazNU named after al-Farabi, 71 al-Farabi ave, 050040, Almaty, Kazakhstan. Researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Khompysh A. – PhD, researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Dyussenbayev D.S. - researcher of Information security laboratories IICT CS MEN RK, st. Shevchenko 28, 050010, Almaty, Kazakhstan.

Поступила в редакцию 24.08.2021