DOI 10.52209/1609-1825_2022_4_411 ӘОЖ 004.421

Жаңа 4 биттік S-блок алу әдісі және алынған S-блокты қатал лавиндік критерийі бойынша зерттеу

[1]***ХОМПЫШ Ардабек,** PhD, ғылыми қызметкер, ardabek@mail.ru,*
*[1]**КАПАЛОВА Нурсулу Алдажаровна,** т.ғ.к., қауымдастырылған профессор, бас ғылыми қызметкер, nkapalova@mail.ru,*
*[2]**САҚАН Қайрат Сақанұлы,** докторант, kairat_sks@mail.ru,*
*[1]**ДЮСЕНБАЕВ Дилмуханбет Самуратович,** ғылыми қызметкер, dimash_dds@mail.ru,*
*[1]**АЛҒАЗЫ Кунболат Тилеуханұлы,** PhD, ғылыми қызметкер, kunbolat@mail.ru,*
[1]Ақпараттық және есептеуіш технологиялар институты, Қазақстан, Алматы, Шевченко көшесі, 28,
[2]«Әл-Фараби атындағы Қазақ ұлттық университеті» КеАҚ, Қазақстан, Алматы, Әл-Фараби даңғылы, 71,
**автор-корреспондент.*

Аңдатпа. *S-блоктарды жасау және олардың криптоберіктілігін зерттеу симметриялы криптографияда негізгі жұмыстардың бірі болып табылады. Себебі симметриялы блокты шифрлау алгоритмдерінің криптоберіктілігіне жауап беретін ең маңызды түрлендірулердің бірі осы S-блок ауыстыру кестесі екендігі белгілі. Осыған байланысты, 4 биттік S-блоктар алуға арналған Галуа өрісіндегі дәрежеге шығару операциясы негізінде жасалған жаңа әдіс жасалынды. Қазіргі уақытта S-блоктың криптоберіктілігін зерттеудің көптеген әдістері бар солардың бірі қатал лавиндік критерийі бойынша зерттеу. Сондықтан жаңа әдіс бойынша алынған S-блоктың криптоберіктілігі Бульдік функциясының қатал лавиндік критерийі (SAC) бойынша зерттелініп алынған нәтижелер танымал алгоритмдердің S-блоктарының нәтижелерімен салыстырылып өте жақсы нәтиже көрсеткен.*

Кілт сөздер: *жеңіл салмақты криптография, қатал лавиндік критерийі (SAC), S-блок, келтірілмейтін көпмүшелік, Бульдік функция,криптоберіктілік, криптография, вектор, P-блок, түрлендіру әдістері, Галуа өрісі, құпия ақпарат.*

Кіріспе

Қазіргі уақытта заманауи технологиялардың дамуына орай интернет желісінде ақпарат алмасу процессі жыл сайын қарқынды дамуымен қатар осы ақпараттың құпиялығынада көңіл бөліне бастағаны белгі. Осы орайда интернет арқылы жүргізілетін құпия ақпараттарды алмасу барысында олардың құпиялылығын сенімді қамтамасыз ету мақсатында криптографиялық әдістер қолданылатыны белгілі. Криптографиялық әдістердің басты мақсаттарының бірі ақпараттың түп нұсқасын қандайда бір математикалық түрлендірулер арқылы ақпараттың мағынасын өзгертумен айналысады [1, 2]. Өздеріңіз білетіндей қазіргі кезде жылдам дамып жатқан сала заттар интернетінің дәуірінде есептеу құрылғылардың қуатылығын арттыру, тиімділігін анықтау екендігін ескерсек, онда «заттар» датчиктері ұрлық дабылдарының, тұрмыстық техниканың және т.б. барлық түрлерінде қолданылады. Бұл құрылғылардың қауіпсіздігін қамтамасыз етуде тиімді шешудің жаңа бағыты – жеңілсалмақты криптография екендігі көптеген шетелдік ғалымдардың еңбектерінен қарауға болады [3, 4]. Осы орайда блоктық шифрлар саласында ең танымал жеңіл салмақты алгоритмдер CLEFIA және PRESENT[5] болып табылады. Екі алгоритм де 2007 жылдан бері белгілі. Бұл жеңіл салмақты блокты шифрларды құрудың негізгі түрлендіру әдістері келесілер: алмастыру әдіс P-блок, ауыстыру әдісі S-блок, цикльдық жылжыту, модулі 2 бойынша қосу операциясы (XOR немесе ⊕) [6]. Бұл түрлендіру әдістерінің ішіндегі S-блок туралы қарастырсақ. S-блок кірісі n-биттен және шығысы m-биттен тұратын ауыстыру блогы. S-блок (ағылшын тілінде substitution-box – ауыстыру блогы) заманауи көптеген блокты шифрларда қолданылатын сызықты емес түрлендіру [7].

S-блок негізінен $m \times n$ өлшемді $Z_2^m \to Z_2^n$ бейнесі. Мысалы: МЕСТ Р 34.13-2015 (Кузнечик) және AES алгоритмдерінде 8x8 өлшемді S-блок қолданса, ал DES алгоритмі 6x4 өлшемді әр түрлі 8 S-блок қолданады [6].

Осыған орай S-блокты алудың көптеген бәсе-

келес әдістері бар, олардың ішінде ең негізгісі математикалық әдіс, себебі онда математиканың заңдылықтарына сәйкес алынғандықтан дифференциальды және сызықты криптоталдауларға кепілдік беретін және шашырау қасиеттерін жақсы орындайды. Қазіргі уақытта жеңіл салмақты криптографиялық алгоритмдердің көбінде 4 биттік S-блок қолданады. Себебі ол өз кезегінде шифрлау жылдамдығын арттыруға мүмкіндік береді. Ақпараттық есептеуіш технологиялар институтының ішіндегі ақпаратттық қауіпсіздік зертханасында орындалып жатқан жоба бойынша жеңіл салмақты алгоритмді құру жұмыстары негізінде, «EM CHIPHER» блокты алгоритмнің [2] модификациясы ретінде жаңа жеңіл салмақты алгоритм жасалынып [8], қазіргі уақытта тиімділігі зерттелінуде. Бұл алгоритмнің негізгі криптоберіктілігіне жауап беретін түрлендіру әдісі S-блок екендігін ескерсек. Онда S-блокты жан жақты зерттеу маңызды болып табылады.

Мақалада осы алгоритмге қолданылған S-блокты алу жолы сипатталып, алынған S-блоктың тиімділігі қатал лавиндік критерийі (SAC), әдістер арқылы зерттелініп нәтижелері ұсынылды.

Жаңа S-блок алу әдісі

Ұсынылып отырған S-блок алу әдісі үш қадамнан тұрады.

Бірінші қадамда $GF(2^4)$ Галуа өрісіндегі мультипликативті топты тудыруші, модуль деп аталатын $P(x)$ келтірілмейтін көпмүшелік және негіз деп аталатын $A(x)$ келтірілмейтін көпмүшелік таңдап алынады. Таңдап алынған $A(x)$ келтірілмейтін көпмүшелікке $P(x)$ модуль бойынша дәрежеге шығару операциясы орындалады:

$$S_i(x) = A(x)^i \bmod P(x), \quad i = \overline{0,15}. \tag{1}$$

Екінші қадамда $S_i(x)$ көпмүшелігінің коэффициенттерін ұзындығы 4-ге тең вектор ретінде қарастырамыз. Егер $S_i'(x) = s_0' + s_1'x + s_2'x^2 + s_3'x^3$ тең болса, онда $S_i' = (s_0', s_1'x, s_2'x^2, s_3'x^3)$ $s_i' \in \{0,1\}$, $i = \overline{0,3}$ тең. Осыдан кейін S_i-ге, ұзындығы әр түрлі тұрақты вектор B модуль 2 (*xor*) қосу операциясы орындалады:

$$S_i' = (S_i \oplus B) \bmod P. \tag{2}$$

Үшінші қадамда (2) формула бойынша алынған вектор элементтері 0 мен 1 тұратын M_{ij} матрицасы бойынша көбейтіледі:

$$S_i'' = M_{ij} \times S_i', \quad i,j = \overline{0,3}. \tag{3}$$

(3) формула бойынша есептеліп алынған екілік жүйедегі мәндерді ондық жүйеге аудару арқылы 1-кестедегідей S-блоктың мәндерін анықтаймыз.

Зерттеу әдіснамасы

S-блоктың криптоберіктілігін зерттеудің көптеген танымал әдістері бар, солардың ішінде біздің қарастырып отырған әдіс қатал лавиндік критерийі (SAC). Енді осы 1-кестеде көрсетілген S-блоктың беріктілігін осы әдіс бойынша зерттеу үшін, әдістің сипаттамаларына тоқталсақ.

S-блокты қатал лавиндік эффекті қасиетіне зерттеу

Бульдік функциясының қатал лавиндік критерийінің (SAC) бірі шифрлау алгоритміндегі түрлендірулерін құру процесінде Шеннон принциптеріне сәйкес шашырату принципін бейнелесе, екінші жағынан дифференциалды криптоталдауға төзімділікті анықтайтын S-блокты құру процесінде кеңінен пайдаланылады. Сондықтан бульдік функцияларды S-блоктың құрылымының бөлігі ретінде сипаттауға болады. SAC қанағаттандыратын бульдік функцияларға негізделген S-блоктарының құрылымы жайлы [9-13] ғалымдардың еңбектерінде айтылған. Бульдік функцияның қатал лавиндік критерийін зерттеу келесі белгілеулер, ұғымдар мен анықтамаларға негізделген.

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 $F(x)$-ті мына түрде анықтаймыз: $F: F_2^n \longmapsto F_2^m$.

Анықтама-1. $F(x) = (f_1, f_2, \ldots, f_m)$ функциясының $f_1, f_2, \ldots, f_m$ – бульдік функциялары F бульдік функциясының координаталары деп аталады. $m = 1$ болған кезде векторлы бульдік функция шығысында тек бір бит ғана болатын бульдік функцияға эквивалентті.

Анықтама-2. $f(x): F_2^n \longmapsto F_2$ – n-айнымалы бульдік функция болсын, мұндағы $x = (x_0, x_1, \ldots, x_{n-1})$. Онда $f(x)$ функциясының хемминг салмағы келесідей анықталады:

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

Анықтама-3. $f(x): F_2^n \longmapsto F_2$ бульдік функциясы болса, онда $f(x)$ функциясының $u \in F_2^n$ екілік векторы арқылы алынған өсімшесі келесідей анықтаймыз:

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

Анықтама-4. Қандай да бір бульдік функция $f(x)$ қатал лавиндік критерийді қанағаттандырады, егер $u \in F_2^n$ үшін келесі 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 келесі (7) формуладағыдай өрнектеуге болады:

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

Егер барлық (n,m)-векторлық функциялардың координаталық функциялары қатал лавиндік критерийін орындайтын болса, онда S-блоктың бір кіріс биті ½ ықтималдығымен өзгерген кезде әрбір шығыс биті өзгереді. Демек, шығыс биттерінің жартысы өзгереді деп қарастыруға болады.

Алынған нәтижелер

Енді, негізгі жұмыс S-блоктың қатал лавиндік критерийі бойынша зерттеуге көшейік. Түсінікті болу үшін 1-кестедегі S-блокты декомпозиция арқылы бульдік функция компоненттерімен жазып алайық:

$$S_1 = \begin{Bmatrix} F & 5 & D & 8 & C & 2 & 4 & 7 & 0 & 9 & 6 & A & 1 & 3 & E & B \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{Bmatrix}. \quad (8)$$

Енді, (8)-формуладағы S-блоктың барлық жолдардың компоненттік мәндері негізінде төрт айнымалысы бар ($n=4$) бульдік функциясын қатал лавиндік критерийіне сәйкестігін зерттеуге көшеміз:

$$\begin{aligned} f_1(x_1,x_2,x_3,x_4) &= \{1\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\}, \\ f_2(x_1,x_2,x_3,x_4) &= \{1\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,0\}, \\ f_3(x_1,x_2,x_3,x_4) &= \{0\,1\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\}, \\ f_4(x_1,x_2,x_3,x_4) &= \{0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\}. \end{aligned} \quad (9)$$

Осыдан кейін 3-ші және 4-анықтаманы пайдалана отырып, келесі 2-кестені құрайық. 2-кестеде $f_1(x)$ бульдік функцияның төрт айнымалысының барлық мүмкін мәндеріндегі (9)-формулаға сәйкес нәтижелері, $f_1(x)$ бульдік функцияның $hw(u)=1$ өсімшесімен қосылған аргументіндегі мәні және $D_u f_1(x)$ өсімшесінің нәтижелері көрсетілген.

Енді, (9)-формуланы пайдаланып, осындай есептеулерді біз S-блоктың екінші, үшінші және төртінші жолдың компоненттік мәндері үшін жүргіземіз. Нәтижелері 3,4,5-кестелерде көрсетілген.

1-кесте – S-блоктың мәндері

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
F	5	D	8	C	2	4	7	0	9	6	A	1	3	E	B

2-кесте – Берілген $f_1(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_1(x)$	$f_1(x\oplus0001)$	$D_{0001}f_1(x)$	$f_1(x\oplus0010)$	$D_{0010}f_1(x)$	$f_1(x\oplus0100)$	$D_{0100}f_1(x)$	$f_1(x\oplus1000)$	$D_{1000}f_1(x)$
f(0000)=1	f(0001)=1	0	f(0010)=1	0	f(0100)=0	1	f(1000)=0	1
f(0001)=1	f(0000)=1	0	f(0011)=0	1	f(0101)=0	1	f(1001)=1	0
f(0010)=1	f(0011)=0	1	f(0000)=1	0	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)=0	0	f(0110)=0	0	f(0000)=1	1	f(1100)=1	1
f(0101)=0	f(0100)=0	0	f(0111)=1	1	f(0001)=1	1	f(1101)=1	1
f(0110)=0	f(0111)=1	1	f(0100)=0	0	f(0010)=1	1	f(1110)=0	0
f(0111)=1	f(0110)=0	1	f(0101)=0	1	f(0011)=0	1	f(1111)=1	0
f(1000)=0	f(1001)=1	1	f(1010)=0	0	f(1100)=1	1	f(0000)=1	1
f(1001)=1	f(1000)=0	1	f(1011)=0	1	f(1101)=1	0	f(0001)=1	0
f(1010)=0	f(1011)=0	0	f(1000)=0	0	f(1110)=0	0	f(0010)=1	1
f(1011)=0	f(1010)=0	0	f(1001)=1	1	f(1111)=1	1	f(0011)=0	0
f(1100)=1	f(1101)=1	0	f(1110)=0	1	f(1000)=0	1	f(0100)=0	1
f(1101)=1	f(1100)=1	0	f(1111)=1	0	f(1001)=1	0	f(0101)=0	1
f(1110)=0	f(1111)=1	1	f(1100)=1	1	f(1010)=0	0	f(0110)=0	0
f(1111)=1	f(1110)=0	1	f(1101)=1	0	f(1011)=0	1	f(0111)=1	0
	$\sum D_{0001}f_1(x)=8$		$\sum D_{0010}f_1(x)=8$		$\sum D_{0100}f_1(x)=12$		$\sum D_{1000}f_1(x)=8$	

3-кесте – Берілген $f_2(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_2(x)$	$f_2(x \oplus 0001)$	$D_{0001}f_2(x)$	$f_2(x \oplus 0010)$	$D_{0010}f_2(x)$	$f_2(x \oplus 0100)$	$D_{0100}f_2(x)$	$f_2(x \oplus 1000)$	$D_{1000}f_2(x)$
f(0000)=1	f(0001)=0	1	f(0010)=0	1	f(0100)=1	1	f(1000)=0	1
f(0001)=0	f(0000)=1	1	f(0011)=0	0	f(0101)=0	0	f(1001)=0	0
f(0010)=0	f(0011)=0	0	f(0000)=1	1	f(0110)=1	1	f(1010)=1	1
f(0011)=0	f(0010)=0	0	f(0001)=0	0	f(0111)=1	1	f(1011)=1	1
f(0100)=0	f(0101)=1	1	f(0110)=0	0	f(0000)=1	1	f(1100)=0	0
f(0101)=1	f(0100)=0	1	f(0111)=1	0	f(0001)=1	1	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	0	f(1111)=1	0
f(1000)=0	f(1001)=0	0	f(1010)=1	1	f(1100)=0	0	f(0000)=1	1
f(1001)=0	f(1000)=0	0	f(1011)=1	1	f(1101)=0	0	f(0001)=0	0
f(1010)=1	f(1011)=1	0	f(1000)=0	1	f(1110)=1	1	f(0010)=0	1
f(1011)=1	f(1010)=1	0	f(1001)=0	1	f(1111)=0	0	f(0011)=0	1
f(1100)=0	f(1101)=1	1	f(1110)=1	1	f(1000)=0	0	f(0100)=0	0
f(1101)=1	f(1100)=0	1	f(1111)=1	0	f(1001)=0	0	f(0101)=1	0
f(1110)=1	f(1111)=1	0	f(1100)=0	1	f(1010)=1	1	f(0110)=0	1
f(1111)=1	f(1110)=1	0	f(1101)=1	0	f(1011)=0	0	f(0111)=1	0
	$\sum D_{0001}f_2(x)=8$		$\sum D_{0010}f_2(x)=8$		$\sum D_{0100}f_2(x)=8$		$\sum D_{1000}f_2(x)=8$	

4-кесте – Берілген $f_3(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_3(x)$	$f_3(x \oplus 0001)$	$D_{0001}f_3(x)$	$f_3(x \oplus 0010)$	$D_{0010}f_3(x)$	$f_3(x \oplus 0100)$	$D_{0100}f_3(x)$	$f_3(x \oplus 1000)$	$D_{1000}f_3(x)$
f(0000)=1	f(0001)=1	0	f(0010)=1	0	f(0100)=1	0	f(1000)=0	1
f(0001)=1	f(0000)=1	0	f(0011)=0	1	f(0101)=0	1	f(1001)=0	1
f(0010)=1	f(0011)=0	1	f(0000)=1	0	f(0110)=1	0	f(1010)=1	0
f(0011)=0	f(0010)=1	1	f(0001)=1	1	f(0111)=1	1	f(1011)=0	0
f(0100)=1	f(0101)=0	1	f(0110)=1	0	f(0000)=1	0	f(1100)=0	1
f(0101)=0	f(0100)=1	1	f(0111)=1	1	f(0001)=1	1	f(1101)=0	0
f(0110)=1	f(0111)=1	0	f(0100)=1	0	f(0010)=1	0	f(1110)=1	0
f(0111)=1	f(0110)=1	0	f(0101)=0	1	f(0011)=0	1	f(1111)=0	1
f(1000)=0	f(1001)=0	0	f(1010)=1	1	f(1100)=0	0	f(0000)=1	1
f(1001)=0	f(1000)=0	0	f(1011)=0	0	f(1101)=0	0	f(0001)=1	1
f(1010)=1	f(1011)=0	1	f(1000)=0	1	f(1110)=1	0	f(0010)=1	0
f(1011)=0	f(1010)=1	1	f(1001)=0	0	f(1111)=0	0	f(0011)=0	0
f(1100)=0	f(1101)=0	0	f(1110)=1	1	f(1000)=0	0	f(0100)=1	1
f(1101)=0	f(1100)=0	0	f(1111)=0	0	f(1001)=0	0	f(0101)=0	0
f(1110)=1	f(1111)=0	1	f(1100)=0	1	f(1010)=1	0	f(0110)=1	0
f(1111)=0	f(1110)=1	1	f(1101)=0	0	f(1011)=0	0	f(0111)=1	1
	$\sum D_{0001}f_3(x)=8$		$\sum D_{0010}f_3(x)=8$		$\sum D_{0100}f_3(x)=4$		$\sum D_{1000}f_3(x)=8$	

Соңында S-блоктың барлық жолдарының компоненттері арқылы алынған нәтижелерді (10) формуладағыдай матрица түрінде өрнектейік:

$$K_S = \begin{pmatrix} \sum D_{0001}f_1(x) & \sum D_{0010}f_1(x) & \sum D_{0100}f_1(x) & \sum D_{1000}f_1(x) \\ \sum D_{0001}f_2(x) & \sum D_{0010}f_2(x) & \sum D_{0100}f_2(x) & \sum D_{1000}f_2(x) \\ \sum D_{0001}f_3(x) & \sum D_{0010}f_3(x) & \sum D_{0100}f_3(x) & \sum D_{1000}f_3(x) \\ \sum D_{0001}f_4(x) & \sum D_{0010}f_4(x) & \sum D_{0100}f_4(x) & \sum D_{1000}f_4(x) \end{pmatrix} = \begin{pmatrix} 8 & 8 & 12 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 4 & 8 \\ 8 & 8 & 8 & 12 \end{pmatrix}. \quad (10)$$

Нәтижелерді талқылау

Ұсынылып отырған мақаладағы жаңа S-блок алу әдісі негізінде алынған S-блок алмастырулар қатал лавиндік әсерді (SAC) өте жақсы нәтиже көрсеткендігін (10)-формуладағы мәндерден көруге болады. Себебі қатал лавиндік әсерді (SAC) орындау үшін олар $\frac{N}{2}=8$ саны маңында болуы тиіс, мұндағы $N=2^4$. Дәл осындай есептеу жолымен біз заманауи блокты Serpent, HB-1 (Hummingbird-1), HB-2 (Hummingbird-2) шифрларында қолданатын отырған S_1-блок, S_2-блок және S_3-блоктарға (6-кесте) зерттеу жүргізіп төмендегідей нәтижелер алдық:

$$K_{S1}=\begin{pmatrix}12&12&8&8\\8&12&8&8\\12&8&12&8\\8&12&8&12\end{pmatrix},\quad K_{S2}=\begin{pmatrix}8&12&12&8\\12&8&12&8\\12&8&12&8\\12&12&8&12\end{pmatrix},\quad K_{S3}=\begin{pmatrix}12&12&8&8\\12&8&8&8\\8&12&12&12\\8&12&8&12\end{pmatrix}. \tag{11}$$

Шетелдік ғалым M.O. Saarinen және т.б. ғалымдардың еңбектерінде бұл S-блоктарды «Алтын S-блоктар» деп атаған [14, 15].

Біздің ұсынып отырған S-блок (11) формуладағы мәндермен салыстырғанда өте жоғары нәтиже көрсеткенін көріп отырмыз.

Қорытынды

Ұсынылып отырған жаңа S-блок алу әдісі Галуа өрісіндегі дәрежеге шығару операциясы негізінде алынып отыр. Қазіргі симметриялы блокты шифрларда қолданылатыны S-блоктың маңыздылығын ескерсек, онда бұл әдіс арқылы жоғары сапалы S-блокты алу үшін әркім өз қалауы бойынша қажетті аргументтерді, яғни келтірілмейтін көпмүшелікті, негізді, векторды және M массивін өзгерту арқылы қалаған S-блокты ала алады. Жаңа S-блок алу әдісі арқылы бірнеше S-блоктар алынып қатал лавиндік әсері (SAC) тексеріліп өте жақсы нәтиже көрсеткені дәлелденді. Тексерілген S-блоктардың ішінде тек біреуінің ғана нәтижесі осы мақалада ұсынылды.

Алынған S-блоктың беріктілігі дифференциальды талдау әдістері бойынша жүргізіліп өте жақсы нәтиже көрсетілді.

5-кесте – Берілген $f_4(x)$ бульдік функциясының өсімшелердің мәндерін анықтау

$f_4(x)$	$f_4(x\oplus0001)$	$D_{0001}f_4(x)$	$f_4(x\oplus0010)$	$D_{0010}f_4(x)$	$f_4(x\oplus0100)$	$D_{0100}f_4(x)$	$f_4(x\oplus1000)$	$D_{1000}f_4(x)$
f(0000)=1	f(0001)=0	1	f(0010)=1	0	f(0100)=1	0	f(1000)=0	1
f(0001)=0	f(0000)=1	1	f(0011)=1	1	f(0101)=0	0	f(1001)=1	1
f(0010)=1	f(0011)=1	0	f(0000)=1	0	f(0110)=0	1	f(1010)=0	1
f(0011)=1	f(0010)=1	0	f(0001)=0	1	f(0111)=0	1	f(1011)=1	0
f(0100)=1	f(0101)=0	1	f(0110)=0	1	f(0000)=1	0	f(1100)=0	1
f(0101)=0	f(0100)=1	1	f(0111)=0	0	f(0001)=0	0	f(1101)=0	0
f(0110)=0	f(0111)=0	0	f(0100)=1	1	f(0010)=1	1	f(1110)=1	1
f(0111)=0	f(0110)=0	0	f(0101)=0	0	f(0011)=1	1	f(1111)=1	1
f(1000)=0	f(1001)=1	1	f(1010)=0	0	f(1100)=0	0	f(0000)=1	1
f(1001)=1	f(1000)=0	1	f(1011)=0	0	f(1101)=0	1	f(0001)=0	1
f(1010)=0	f(1011)=1	1	f(1000)=1	0	f(1110)=1	1	f(0010)=1	1
f(1011)=1	f(1010)=0	1	f(1001)=1	0	f(1111)=1	0	f(0011)=1	0
f(1100)=0	f(1101)=0	0	f(1110)=1	1	f(1000)=0	0	f(0100)=1	1
f(1101)=0	f(1100)=0	0	f(1111)=0	1	f(1001)=1	1	f(0101)=0	0
f(1110)=1	f(1111)=1	0	f(1100)=0	1	f(1010)=0	1	f(0110)=0	1
f(1111)=1	f(1110)=1	0	f(1101)=1	1	f(1011)=1	0	f(0111)=0	1
	$\sum D_{0001}f_4(x)=8$		$\sum D_{0010}f_4(x)=8$		$\sum D_{0100}f_4(x)=8$		$\sum D_{1000}f_4(x)=12$	

6-кесте – «Алтын S-блоктар»

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

Жұмыс AP09259570 «Шектелген ресурстар үшін отандық жеңілсалмақты шифрлау алгоритмін құру және зерттеу» гранттық қаржыландыру ғылыми жобасы аясында жүргізілді.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.
2. Kapalova N., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform // Cogent engineering. – 2020. – Vol. 7 (178829). – ISSN 2331-1916. – pp. 1-12.
3. Preneel B. Perspectives on Lightweight Cryptography, Inscript 2010, Shanghai, China, 20-24 October 2010.
4. P. Israsena. Securing ubiquitous and low-cost RFID using tiny encryption algorithm. In 1-st International Symposium on Wireless Pervasive Computing, 2006, pages 4. IEEE, 2006.
5. Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. 9. International Workshop on Cryptographic Hardware and Embedded Systems // CHES 2007, Vienna, Austria, LNCS, Springer-Verlag, September 10-13, 2007. – 18 p.
6. Хомпыш А. Криптостойкости S-блоков в алгоритме шифрования на основе EM // «Наука XXI века: новый подход»: Матер. XXIII молодёжной межд. науч.-практ. конф. студентов, аспирантов и молодых учёных. – Санкт-Петербург, 2019. – С. 15-19.
7. Долгов В.И., Кузнецов А.А., Лисицкая И.В. и др. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров // Прикладная радиоэлектроника. Том 8. № 3. 2009. С. 268-276.
8. Капалова Н.А., Хомпыш А., Дюсенбаев Д.С., Сулейменов О.Т. Исследование «лавинного эффекта» разработанного алгоритма шифрования // IV Международная научно-техническая конференция «Минские научные чтения-2021». Том 3. 09 декабря 2021 г. Минск, Беларусь, С. 238-244.
9. Pasalic E., Johansson T., Maitra S., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity. Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.
10. Shah, T. Hussain, I. Gondal, M.A. Mahmood, H. Statistical analysis of S-box in image encryption applications based on majority logic criterion. Int. J. Phys. Sci. 2011, 6, 4110-4127.
11. A.H. Zahid, and M.J. Arshad, «An innovative design of substitution-boxes using cubic polynomial mapping», Symmetry, vol. 11, no. 3, p. 437, 2019.
12. A.H. Zahid, E. Al-Solami and M. Ahmad, «A Novel Modular Approach Based Substitution-Box Design for Image Encryption», in IEEE Access, vol. 8, pp. 150326-150340, 2020.
13. Carlet C. Vectorial Boolean functions for // CambridgeUniv. Press, Cambridge. – 95 p. [Электронный ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf
14. Saarinen, Markku-Juhani O. «Cryptographic Analysis of All 4 x 4 – Bit S-Boxes». IACR Cryptol. ePrint Arch. 2011 (2011): 218.
15. Ghoshal, A., Sadhukhan, R., Patranabis, S., Datta, N., Picek, S., & Mukhopadhyay, D. (2018). Lightweight and Side-channel Secure 4 × 4 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.

Новый метод проектирования 4-битного S-блока и исследования его результатов на строгий лавинный критерий

*[1]**ХОМПЫШ Ардабек,** PhD, научный сотрудник, ardabek@mail.ru,*
*[1]**КАПАЛОВА Нурсулу Алджаровна,** к.т.н., ассоциированный профессор, главный научный сотрудник, nkapalova@mail.ru,*
*[2]**САКАН Кайрат Саканулы,** докторант, kairat_sks@mail.ru,*
*[1]**ДЮСЕНБАЕВ Дилмуханбет Самуратович,** научный сотрудник, dimash_dds@mail.ru,*
*[1]**АЛГАЗЫ Кунболат Тилеуханулы,** PhD, научный сотрудник, kunbolat@mail.ru,*
[1]Институт информационных и вычислительных технологий, Казахстан, Алматы, ул. Шевченко, 28,
[2]НАО «Казахский национальный университет имени Аль-Фараби», Казахстан, Алматы, пр. Аль-Фараби, 71,
**автор-корреспондент.*

***Аннотация.** Создание S-блоков и исследование их криптостойкости является одним из основных направлений деятельности в симметричной криптографии. Известно, что одним из наиболее важных преобразований, отвечающих за криптографическую стойкость симметричного блочного алгоритма шифрования, является таблица замены S-блоков. В связи с этим, в данной работе рассматривается новый метод получения 4-битных S-блоков, основанный на операции возведения в степень в поле Галуа. В настоящее время существует большое количество методов проверки криптостойкости S-блоков, одним из которых является исследование строгого лавинного критерия. Поэтому исследование криптостойкости S-блока, полученного новым методом на основе строгого лавинного критерия (SAC) булевой функции в сравнении с результатами S-блоков популярных алгоритмов, показало очень хорошие результаты.*

***Ключевые слова:** легковесная криптография, строгий лавинный критерий (SAC), S-блок, неприводимый поли-*

ном, булева функция, криптостойкость, криптография, вектор, P-блок, методы преобразования, поле Галуа, конфиденциальная информация.

A New Method for Designing a 4-bit S-block and Studying Its Results for a Strict Avalanche Criterion

[1]***KHOMPYSH Ardabek,** PhD, Researcher, ardabek@mail.ru,*
[1]***KAPALOVA Nursulu,** Cand. of Tech. Sci., Associate Professor, Chief Researcher, nkapalova@mail.ru,*
[2]***SAKAN Kairat,** doctoral student, kairat_sks@mail.ru,*
[1]***DYUSSENBAYEV Dilmukhanbet,** Researcher, dimash_dds@mail.ru,*
[1]***ALGAZY Kunbolat,** PhD, Researcher, kunbolat@mail.ru,*
[1]Institute of Information and Computational Technologies, Kazakhstan, Almaty, Shevchenko Street, 28,
[2]NPJSC «Al-Farabi Kazakh National University», Kazakhstan, Almaty, Al-Farabi Avenue, 71,
**corresponding author.*

***Abstract.** The creation of S-boxes and the study of their cryptographic strength is one of the main activities in symmetric cryptography. It is known that one of the most important transformations responsible for the cryptographic strength of a symmetric block encryption algorithm is the S-box replacement table. In this regard, in this paper, we consider a new method for obtaining 4-bit S-boxes based on the exponentiation operation in the Galois field. Currently, there are a large number of methods for checking the cryptographic strength of S-boxes, one of which is the study of a strict avalanche criterion. Therefore, the study of cryptographic strength of the S-box obtained by the new method based of a strict avalanche criterion (SAC) of a Boolean function in comparison with the results of S-boxes of popular algorithms, showed very good results.*

***Keywords:** lightweight cryptography, strict avalanche criterion (SAC), S-box, irreducible polynomial, boolean function, cryptographic strength, cryptography, vector, P-block, transformation methods, Galois field, confidential information.*

REFERENCES

1. Babenko L.K., Ishhukova E.A. Sovremennye algoritmy blochnogo shifrovanija i metody ih analiza [Modern block cipher algorithms and methods for their analysis]. – Moscow: Gelios ARV, 2006. – 376 p.
2. Kapalova N., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform // Cogent engineering. – 2020. – Vol. 7 (178829). – ISSN 2331-1916. – pp. 1-12.
3. Preneel B. Perspectives on Lightweight Cryptography, Inscript 2010, Shanghai, China, 20-24 October 2010.
4. P. Israsena. Securing ubiquitous and low-cost RFID using tiny encryption algorithm. In 1-st International Symposium on Wireless Pervasive Computing, 2006, pages 4. IEEE, 2006.
5. Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. 9. International Workshop on Cryptographic Hardware and Embedded Systems // CHES 2007, Vienna, Austria, LNCS, Springer-Verlag, September 10-13, 2007. – 18 p.
6. KHompysh A. Kriptostojkosti S-blokov v algoritme shifrovanija na osnove EM [Security of S-boxes in an EM-based encryption algorithm] «Nauka XXI veka: novyj podhod»: Mater. XXIII molodjozhnoj mezhd. nauch.-prakt. konf. studentov, aspirantov i molodyh uchjonyh. – Saint Petersburg, 2019. – pp. 15-19.
7. V.I. Dolgov, A.A. Kuznecov, I.V. Lisickaja i dr. Issledovanie kriptograficheskih svojstv nelinejnyh uzlov zameny umen'shennyh versij nekotoryh shifrov [Investigation of cryptographic properties of non-linear substitution nodes of reduced versions of some ciphers] // Prikladnaja radiojelektronika. Tom 8. No. 3. 2009. pp. 268-276.
8. Kapalova N.A., KHompysh A., Dyusenbaev D.S., Suleimenov O.T. Issledovanie «lavinnogo jeffekta» razrabotannogo algoritma shifrovanija [Study of the «avalanche effect» of the developed encryption algorithm] // IV Mezhdunarodnaja nauchno-tehnicheskaja konferencija «Minskie nauchnye chtenija-2021». Tom 3. 09 dekabrja 2021 g. Minsk, Belarus', pp. 238-244.
9. Pasalic E., Johansson T., Maitra S., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity. Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.
10. Shah, T. Hussain, I. Gondal, M.A. Mahmood, H. Statistical analysis of S-box in image encryption applications based on majority logic criterion. Int. J. Phys. Sci. 2011, 6, 4110-4127.
11. A.H. Zahid, and M.J. Arshad, «An innovative design of substitution-boxes using cubic polynomial mapping», Symmetry, vol. 11, no. 3, p. 437, 2019.
12. A.H. Zahid, E. Al-Solami and M. Ahmad, «A Novel Modular Approach Based Substitution-Box Design for Image Encryption», in IEEE Access, vol. 8, pp. 150326-150340, 2020.
13. Carlet C. Vectorial Boolean functions for // CambridgeUniv. Press, Cambridge. – 95 p. [Электронный ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf
14. Saarinen, Markku-Juhani O. «Cryptographic Analysis of All 4 x 4 – Bit S-Boxes». IACR Cryptol. ePrint Arch. 2011 (2011): 218.
15. Ghoshal, A., Sadhukhan, R., Patranabis, S., Datta, N., Picek, S., & Mukhopadhyay, D. (2018). Lightweight and Side-channel Secure 4 × 4 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