ӘОЖ 44.31.35 **DOI 10.52167/1609-1817-2024-134-5-292-304**

Н.А. Капалова✉, С.Е. Нысанбаева, Д.С. Дюсенбаев, А. Хомпыш
ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан
E-mail: Kapalova@ipic.kz

AL04 ШИФРЛАУ АЛГОРИТМІН ҚҰРУ ЖӘНЕ ОНЫҢ КРИПТОГРАФИЯЛЫҚ ҚАСИЕТТЕРІН ЗЕРТТЕУ

Аңдатпа. Кез келген радиобайланыс құралдары арқылы жүргізілетін келіссөздер табиғаты бойынша құпия бола алмайды, өйткені оларды мүдделі тараптар ұстап алуы мүмкін. Радиобайланысты қорғау өзекті мәселе болғандықтан, радиобайланыс жүйесін ақпаратты криптографиялық қорғау модулімен қайта жабдықтау шешімі ұсынылды, ол функционалды түрде жеке корпуста жүзеге асырылып, радиостанция мен сөйлесу түймесінің (тангента) ортасына қосылатын болады. Жасалып жатқан ақпаратты криптографиялық қорғау құралдары толығымен отандық өнім болып табылады. Ақпаратты шифрлау алгоритмі мен құрылымдық шешімдер ақпараттық қауіпсіздік талаптарына сәйкес келеді және ҚР СТ 1073-2007 мемлекеттік стандарты бойынша сертификаттау үшін «ашық» болады. Ақпараттық қауіпсіздік модулі үшін жаңа шифрлау алгоритмі AL04 құрылды. Бұл жұмыста осы алгоритмнің сипаттамасы және оның криптографиялық қасиеттерін бағалау нәтижелері берілген. AL04 негізгі параметрлері: блок ұзындығы – 128 бит; кілт ұзындығы – 128 бит; раундтардың саны – 8.

Жұмыс барысында әртүрлі криптоталдау әдістерін пайдалана отырып құрылған шифрлау алгоритмінің қауіпсіздігін бағалау нәтижелері алынды. Атап айтқанда, әзірленген шифрлау алгоритмі сызықтық және дифференциалды криптоанализге төзімділіктің қажетті деңгейін қамтамасыз ететіні көрсетілді. Сонымен қатар, толық алгоритмнің сызықтық криптоталдауы жүргізілді және AL04 шифрлау алгоритмі криптоталдаудың осы түріне қарсы қауіпсіздіктің жоғары деңгейін көрсетті. AL04 шифрлау алгоритміне алгебралық криптоталдау жүргізілді. Зерттеу нәтижелерін сараптай келе, ұсынылған алгоритм қажетті криптографиялық қасиеттерді көрсететіні анықталды.

Түйінді сөздер. Криптографиялық беріктілік, дифференциалдық криптоталдау, сызықтық криптоталдау, алгебралық криптоталдау.

Кіріспе.

Заманауи криптография көптеген салаларда ақпаратты қорғау үшін қолданылады, соның ішінде қаржылық транзакциялар, онлайн байланыстар, деректерді сақтау және т.б. Криптография желінің қауіпсіздігін қамтамасыз ету үшін өте маңызды болып саналатын ақпараттың құпиялылығын, тұтастығын және түпнұсқалығын қамтамасыз етуге мүмкіндік береді. Бұған әртүрлі криптографиялық алгоритмдерді қолдану арқылы қол жеткізіледі.

Осылайша, заманауи криптография әлемдегі ақпараттық қауіпсіздікті қамтамасыз етуде шешуші рөл атқарады және оның маңыздылығы болашақта да арта бермек.

Криптографияның барлық нақты міндеттері көбінесе технологияның даму деңгейіне, қолданылатын байланыс құралдарына және ақпаратты беру әдістеріне байланысты [1]. Мысалы, криптотұрақты блоктық шифр белгілі бір шарттарды қанағаттандыруы керек. Бұл шарттар [2] жұмыста қарастырылған, және де шифрлау теориясында негізгі талаптар болып табылады. Криптоталдауға төзімді шифрдың араластыру және шашырату қасиеттері болуы керек. Араластыру – шифрланған мәтін мен кілт арасындағы қатынасты жасырады, ал шашырату шифрланған мәтін мен ашық мәтін арасындағы байланысты жасырады. Блоктық шифрларға қойылатын талаптарды

қанағаттандыру үшін қазіргі шифрлау алгоритмдері әртүрлі криптографиялық түрлендірулерді пайдаланады.

Заманауй талаптарға сай, күрделі зерттеулерден кейін SP желілік құрылымы бар жаңа алгоритмдер буыны пайда болды. Бұл алгоритмдердің жалпы құрылымы алмастыру-орналастыру желісінің (SP желісі) нұсқасы болып табылады. Желінің мұндай құрылымы ауыстыру деңгейінен (сызықты емес элементтер), сызықтық (аралас) қабаттан және кілтті қосу қабатынан тұратын, қайталанатын түрлендіруді пайдаланады. Аталмыш құрылым әрбір итерацияда (айналымда) бүкіл деректер блогын түрлендіреді және Feistel желісімен салыстырғанда кіріс векторын әлдеқайда жылдам араластырады. Бұл көрсеткіш сызықтық қабатта MDS матрицасын (Maximal Distance Separable matrix) пайдалану арқылы күшейтіледі. Мұндай матрица шығыс векторының биттерінің кіріс биттеріне мүмкін болатын тәуелділігін жоюды қамтамасыз етеді және көптеген белгілі шифрлау алгоритмдерінде сызықтық түрлендірулер ретінде қолданылады [3].

[4]-ші жұмыста авторлар алмастыру-орналастыру желісінің (SPN) блоктық шифрларының интегралдық қасиетін, қысқартылған және мүмкін емес дифференциалдарын бағалаудың жаңа әдісін ұсынды. Бұл әдіс тек қысқартылған алгоритмдер үшін сыналған.

Симметриялық блокты алгоритмдер сызықтық түрлендіру ретінде жақсы тексерілген МДР түрлендіруін пайдаланады. Бұл түрлендіру ең жақсы дисперсиялық қасиеттерді береді. МДР кодтары (максималды қашықтықпен бөлінетін кодтар) негізінен бастапқы мәтін векторын қандай да бір тұрақтылардың матрицасына көбейту үшін қолданылады, оны әдетте МДР матрицасы деп атайды [5]. Белгілі алгоритмдердің ішкі кілттерін (раундық кілттерді) генерациялау схемасының келесі кемшіліктері бар:

– басты кілтті бір ішкі кілт арқылы қалпына келтіру мүмкіндігі;

– ішкі кілттер арасындағы жеткілікті қарапайым тәуелділіктер (байланысты кілттер шабуылына осалдылығы);

– ішкі кілттердің біріншісі – басты кілт болуы;

– басты кілт биттерінің өзгерістерінің бірінші ішкі кілттердің биттеріне әлсіз әсері;

– орналастыру схемасында циклдік функциядан өзгеше басқа құрылымды пайдалануы;

– шифрлау және шифрды шешу үшін ішкі кілттер тізбегін құрудың әртүрлі күрделілігі.

Осыған байланысты симметриялық блокты шифрлау алгоритмін жасау кезінде жоғарыда аталған криптографиялық процедуралардың ерекшеліктері ескерілетін болады. Әдетте, жаңа алгоритм құру немесе бар шифрлау алгоритмін өзгерту кезінде алдымен оның қасиеттері талданады.

Құрастырылған алгоритмдерді жүзеге асыру мәселесі де маңызды. Мысалы, әскери салада коммуникациялық қауіпсіздіктің негізгі бағыттарының бірі шифрлау жабдықтарын (құрылғыларын) пайдалану болып табылады. Бұл құпияның кез келген жіктемесі бар ақпаратты өтудің барлық кезеңдерінде және басқарудың барлық деңгейлерінде кепілді жасыруға мүмкіндік береді.

Радиобайланысты қорғау мәселесін қарастыру кезінде мынадай жағдай туындайды: радиостанциялардың әртүрлі типтерінде сыртқы құрылғыларды қуатпен қамтамасыз ету үшін интерфейстері әртүрлі тангета мен қосқыштарды қолданады. Сонымен қатар көптеген схемалық шешімдерде аппараттық құралға енгізілген ақпаратты криптографиялық қорғау құралдары (АККҚ) бар. Әртүрлі өндірушілердің бұл құралдары бір-бірімен үйлеспейді және өндірушілер шифрлау алгоритмдерінің схемалары мен бастапқы деректерін жарияламайды, бұл жағдай осындай құрылғыларды ҚР СТ 1073-2007 стандартының талаптарына сәйкес сертификаттауға мүмкіндік бермейді.

Осыған байланысты ақпаратты қорғау талаптарына сәйкес келетін және ақпаратты криптографиялық қорғау жүйесінің аппараттық және бағдарламалық бөліктерін сертификаттау үшін «ашық» және толық отандық ақпаратты шифрлау құралын жасау қажет. Бұл өнімді өзіміздің жеке құрастыруымыз жоғары техникалық қызмет көрсетуді, жылдам модернизацияланатын және шетелдік аналогтармен салыстырғанда құны төмен құрал жасауды қамтамасыз етеді.

Радиобайланысты қорғау шешімдерінің бірі функционалды түрде жеке корпуста болатын және радиостанция мен сөйлесу түймесі (тангента) арасындағы саңылауға қосылатын отандық АККҚ құру ұсынылды. Авторлар осы АККҚ үшін жаңа шифрлау алгоритмін құрды. Құрылғыны аппараттық жүзеге асыруды «Гранит» арнайы конструкторлық-технологиялық бюросы ЖШС орындайды. Бұл жұмыста радиобайланысты қорғау үшін қолданылатын шифрлау алгоритмінің құрылымы және әртүрлі криптоталдау әдістерін қолдану арқылы оның сенімділігін зерттеу нәтижелері берілген.

Материалдар мен тәсілдер

Шифрларды құрастыру кезінде олардың беріктігін қамтамасыз ету басты мәселе болып табылады. Криптографиялық алгоритмдердің тұрақтылығын бағалаудың негізгі әдістеріне сызықтық және дифференциалды криптоталдау сияқты шабуылдар жатады. Бұл талдау әдістерін қолдану шифрларды жобалау кезеңінде де оларға шамадан тыс тұрақтылықты орнатуға мүмкіндік береді және осы талдау әдістерін құрастырылған алгоритмге қолдану мүмкіндігін болашақта болдырмайды.

Сызықтық криптоталдаудың мақсаты берілген шифрлау алгоритмі үшін келесі «тиімді» сызықтық өрнекті табу болып табылады:

$$A[i_1, i_2, \dots, i_a] \oplus C[j_1, j_2, \dots, j_b] = K[k_1, k_2, \dots, k_c],$$

мұнда $i_1, i_2, \dots, i_a$, $j_1, j_2, \dots, j_b$ және $k_1, k_2, \dots, k_c$ бекітілген бит позицияларын белгілейді, ал теңдеу еркін берілген ашық мәтін A, сәйкесінше шифрланған мәтін C және кілт K үшін $p \neq 1/2$ ықтималдығымен орындалады.

Сызықтық криптоталдау екі қадаммен жүзеге асырылады. Біріншісі - жоғары ықтималдықпен жарамды ашық мәтін, шифрлық мәтін және кілт арасындағы қатынастарды құру. Екіншісі - кілттік биттерді алу үшін белгілі ашық мәтін - шифрланған мәтін жұптарымен бірге осы қатынастарды пайдалану [6].

Дифференциалды криптоталдау – симметриялық блоктық шифрларды бағалайтын криптоталдау әдістерінің бірі. Бұл әдіс әртүрлі шифрлау раундтарындағы шифрланған мәндер арасындағы айырмашылықтардың түрленуін зерттеуге және зерделеуге негізделген. Шифрланған мәндер арасындағы айырмашылық, әдетте, екі модульді разрядтық қосу операциясын қолдану арқылы алынады [7-8].

Алгебралық криптоталдау криптографиялық алгоритмдердің әлсіз жақтарын табу үшін пайдаланылуы мүмкін, мысалы, S- блоктардағы немесе басқа ішкі математикалық құрылымдардағы осалдықтар. Алгебралық теңдеулер жүйелерін құру арқылы алгоритмдердің қасиеттерін талдауға болады [9].

Криптографиялық алгоритм үшін алгебралық теңдеулер жүйесін құрудың бір жолы - S-блоктардың және алгоритмнің басқа бөліктерін алгебралық теңдеулер түрінде сипаттау. Бұл жағдайда теңдеулер санын азайту үшін тұрақтылық көрсеткіштері жақсы S-блоктарды қолдануға тырысады.

Дегенмен, ақырлы өрістерде алгебралық теңдеулер жүйесін шешудің әмбебап әдістері жоқ екенін атап өткен жөн. Бұл көптеген криптографиялық алгоритмдерге практикалық беріктілігін сақтауға мүмкіндік береді.

Нәтижелер.

Әзірленген AL04 шифрлау алгоритмінің құрылымы жаңа және заманауи талаптарға сай келеді. Алгоритм параметрлері: блок ұзындығы – 128 бит, айналымдар саны – 8, алгоритмге сызықты емес функция ретінде қатысатын S-блоктың кіріс және шығысындағы деректер өлшемі – 8 бит. Негізгі кілт ұзындығы да 128 бит. Қолданылатын түрлендірулер: модуль 2 бойынша қосу және ауыстыру S- блогі, сондай-ақ квадраттық матрицаға көбейту арқылы сипатталған түрлендіру болып табылады.

Ұсынылып отырған алгоритм радиобайланысты қорғауға икемделген, ол AL03 [10] алгоритмінің модификациясы болып табылады.

AL04 алгоритмінің негізгі сұлбасы (1-сурет) мен түрлендіру функциялары төменде келтірілгендей. Шифрлау функциясы:

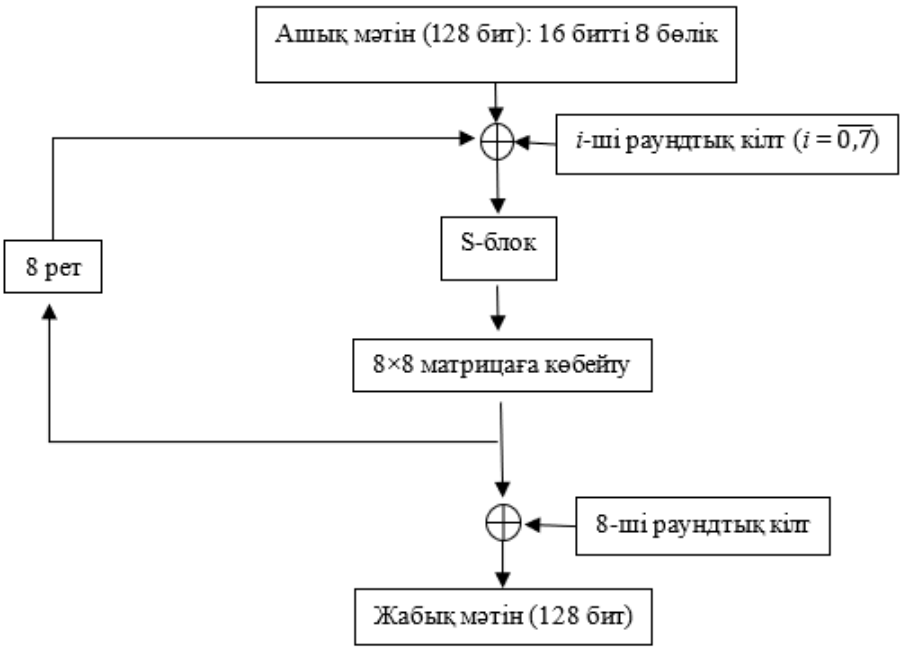
$$\bar{C} = M \otimes \bar{S}(\ldots \bar{S}(M \otimes \bar{S}(\bar{A} \oplus \overline{K_0}) \oplus \overline{K_1}) \ldots \oplus \overline{K_7}) \oplus \overline{K_8}. \quad (1)$$

Дешифрлау функциясы:

$$\bar{A} = \overline{M^{-1}} \otimes \overline{S^{-1}}(\ldots \overline{S^{-1}}(M^{-1} \otimes \overline{S^{-1}}(\bar{C} \oplus \overline{K_8}) \oplus \overline{K_7}) \ldots \oplus \overline{K_1}) \oplus \overline{K_0}, \quad (2)$$

мұндағы квадрат матрица шифрлау немесе дешифрлау кезінде матрицаның өлшеміне қатысты таңдалады. $\bar{A}, \bar{C}, \overline{K_t}$ – векторларының өлшемі $\frac{128}{2^k}$ санына тең, $\bar{S}$ және $\overline{S^{-1}}$ сәйкесінше вектор элементтерінің S-блоктан өту операциясы. $\bar{A}$ – ашық мәтін, $\bar{C}$ – жабық мәтін, $\overline{K_t}$ – раундтық кілттер.

Алгоритмнің ерекшелігі, матрицаның өлшеміне қатысты $GF\left(2^{2^k}\right)/p(x)$ сақинасының элементтері алынады. Алгоритмді k=4 және $p[x] = x^{15} + x^5 + x^4 + x^3 + 1$ мәндерін қабылдаған жағдайды қарастырайық, яғни 8×8 матрица қолданылады. Бұл парамердің таңдалу себебі, шифрлеу функциясына қатысты ең тиімдісі.



1 сурет - AL04 алгоритмінің схемасы

Элементері $\frac{GF(2^{16})[x]}{p[x]}$, $p[x] = x^{15} + x^5 + x^4 + x^3 + 1$ (10000000000111001) сақинасында жататын 8×8 матрица:

CF 98 74 BF 93 8E F2 F3 0A BF F6 A9 EA 8E 4D 6E
6E 20 C6 DA 90 48 89 9C C1 64 B8 2D 86 44 D0 A2
A2 C8 87 70 68 43 1C 2B A1 63 30 6B 9F 30 E3 76
76 33 10 0C 1C 11 D6 6A A6 D7 F6 49 07 14 E8 72
72 F2 6B CA 20 EB 02 A4 8D D4 C4 01 65 DD 4C 6C
6C 76 EC 0C C5 BC AF 6E A3 E1 90 58 0E 02 C3 48
48 D5 62 17 06 2D C4 E7 D5 EB 99 78 52 F5 16 7A
7A E6 4E 1A BB2E F1BE D4AF 37B1 D42A 6EB8

Кері матрица:

99 03 37 0C C6 39 AC 70 B0 42 69 2B 5E 56 9E 74
67 D1 C3 58 D9 BE 7B D1 15 45 72 E7 E7 8A B0 74
9B 45 7D 82 71 64 3A 56 B3 5A FA 9C B5 45 38 5C
49 BA 00 C7 34 AF 23 5D 5D 30 DD 8A 85 74 01 D0
E0 3D 08 DB 46 B4 5A E9 8D 6C F0 76 65 D2 82 22
41 9F AB 5E A7 61 01 79 89 AC CC 0A FE F6 BA 13
B9 EF 21 BB 9C 69 DD BE 64 77 FB C2 40 37 1F 18
21 A0 1C 1 A B9 5D 06 FF 79 7E EB 3F 92 43 42 C8

Сызықтық емес алмастыру функциясы реттінде, AL01 шифрлау алгориміне қолданылған S-блок таңдалды [11]. Ауыстыру таблицасы және оның кері таблицасы төменде келтірілгендей.

S-блок:

A5 04 A6 A7 F7 C6 A4 12 5F C8 C7 D1 F6 D4 7E 7B
0B EF 13 AD 94 5B 4C 8A 0C FC CE 1C 9B 76 19 F3
21 68 53 96 2D D0 A1 89 3D 9C DA 6D 51 AF E1 E9
A2 E3 09 FE C3 3F AA 1E BA DD 9F 1D 28 54 8E 92
E7 D5 43 33 DE 81 3C 97 32 EC 1F 72 74 CD B3 60
3A 95 39 FA 1A 0E C1 05 DF CC A0 8D 87 58 83 D3
26 FD 86 7C 20 4B 08 36 45 DC 3B 79 22 BE AB 14
2A 03 99 2C 6B E5 F9 5C B0 85 5D B2 30 80 ED DB
57 8F 9D A9 D6 B8 EE 24 CB 84 B7 D8 69 A8 6F 50
BD F1 01 38 F8 40 4E BF 9E 0D 91 C9 7D F4 47 07
B9 63 6E 0F EB 70 D9 6A 7A 2B A3 CF 44 65 F5 00
98 35 C2 41 27 1B 62 AC 67 23 88 10 B6 8C 4D C0
64 3E 5A E8 34 D7 9A 16 B4 29 D2 37 73 F2 6C 46
06 E6 CA C4 EA 7F 18 E0 B5 31 Fb FF 71 17 AE 02
B1 15 25 78 BB F0 61 93 11 4F 56 82 8B 42 59 48
2F E2 66 4A 0A 90 2E 75 BC C5 E4 55 52 77 49 5E

Кері S-блок:

AF 92 DF 71 01 57 D0 9F 66 32 F4 10 18 99 55 A3
BB E8 07 12 6F E1 C7 DD D6 1E 54 B5 1B 3B 37 4A
64 20 6C B9 87 E2 60 B4 3C C9 70 A9 73 24 F6 F0
7C D9 48 43 C4 B1 67 CB 93 52 50 6A 46 28 C1 35

95 B3 ED 42 AC 68 CF 9E EF FE F3 65 16 BE 96 E9
8F 2C FC 22 3D FB EA 80 5D EE C2 15 77 7A FF 08
4F E6 B6 A1 C0 AD F2 B8 21 8C A7 74 CE 2B A2 8E
A5 DC 4B CC 4C F7 1D FD E3 6B A8 0F 63 9C 0E D5
7D 45 EB 5E 89 79 62 5C BA 27 17 EC BD 5B 3E 81
F5 9A 3F E7 14 51 23 47 B0 72 C6 1C 29 82 98 3A
5A 26 30 AA 06 00 02 03 8D 83 36 6E B7 13 DE 2D
78 E0 7B 4E C8 D8 BC 8A 85 A0 38 E4 F8 90 6D 97
BF 56 B2 34 D3 F9 05 0A 09 9B D2 88 59 4D 1A AB
25 0B CA 5F 0D 41 84 C5 8B A6 2A 7F 69 39 44 58
D7 2E F1 31 FA 75 D1 40 C3 2F D4 A4 49 7E 86 11
E5 91 CD 1F 9D AE 0C 04 94 76 53 DA 19 61 33 DB

AL04 алгоритмінің раундтық кілті «PSG1.1» әдісі арқылы алынады, бұл әдіс толығырақ [12] жұмыста баяндалға. Негізгі кілт 128 биттен тұрады. Шифрлау және дешифрлау үрдістері сұлбада келтіргендей (1) және (2) өрнектер арқылы орындалады. Құрылған алгоритмінің криптоберіктілігін бағалау натижелері келесі бөлімде сипатталады.

Дифференциалдық талдау. Құрылған алгоритмнің дифференциальдық криптоталдауға төзімділігін бағалау мақсатында, алгоритмның құрлымына сәйкес әр раунд үшін жеке қарастырып шығайық. Бір раунд үшін кіріс және шығыс айырымдар формуласы:

$$\overline{\triangle C_{i,j}} = M \times \overline{S\left(\overline{\triangle A_{i,j}}\right)}, \tag{3}$$

мұндағы, $\overline{S(\overline{\triangle A_{i,j}})} = \left\{\exists (A_i \oplus A_j), \forall K_l : S(A_i \oplus K_l) \oplus S(A_j \oplus K_l)\right\}$ – қандай да ашық мәтіндердің айырымдарына жабық мәтіндердің жиындары сәйкес қойылады. Берілген (3) теңдеуді шешу үшін келесі тұжырымға жүгінеміз. Яғни жабық мәтінді кері матрицаға көбейткеннен шыққан мән $\overline{S(\overline{\triangle A_{i,j}})}$ жиынның қандай да бір элементтіне сәйкес келеді, ол элемент кілттің мәнін анықтайды. Кілттің мәнін анықтау үшін екіден кем емес ашық және жабық мәтіннің жұптары қажет. Анығырақ айтқанда, келесі теп-теңдік орындалуы тиіс, егер (4)-ті қанағаттандыратын кілт бар болса және ол барлық жұптар үшін ортақ шешім болса ғана кілт бола алады:

$$M^{-1} \times \triangle C_{i,j} \equiv S^k\left(\triangle A_{i,j}\right), \tag{4}$$

мұндағы, «≡» - тепе-теңдігі элемент пен жиынның арасындағы қатынасты көрсетеді, егер элемент жиында жатса, онда теңдік ақиқат, ал шешім сол элемент, яғни кілт болады [13]. Ал егер элемент жиында жатпаса, онда теңдік жалған, яғни шешімі жоқ.

Бірінші раундтағы кіріс және шығыс айырымдарына қатысты кілтті анықтау үшін кемінде үш блок болуы қажет немесе басқаша айтқанда, (4) тепе-теңдігін қанағаттандыратын кемінде екі теңдеулер жүйесі болуы қажет, сонда бірінші раундтан кейін кілтті табу ықтималдылығы 1 болады. Екі раундтан кейін кілтті анықтау арнайы таңдалған үш блоктың өзара айырмаларының сәйкес бір ғана бөлігі нөлден өзгеше, қалғандары нөл болған жағдайда орындалады. Үшінші раундтан бастап кілт табу қиындай түседі.

Үш раундтан кейін кілтті анықтау ықтималдығы $(2^{-12})^8 = 2^{-96}$ тең болады. Төртінші раундтан кейін кілтті анықтау ықтималығы 2^{-192} тең, ал бесінші раундтан кейін

2^{-288}. Алтыншы раундтан кейін кілтті анықтау ықтималдығы 2^{-384} тең болады, ал жетінші раундтан кейін 2^{-480} болғандықтан келесідей тұжырымдама жасаймыз. Қарастырып отырған алгоритмге бесінші раундтан кейін дифференциалдық талдау жасау көрсеткіші кілтті толық теруден жоғары, сондықтан алгоритм дифференциалды криптоталдау әдісіне төзімді деп саналады.

Сызықтық талдау. Қарастырып отырған S-блоктың сызықтық талдауы - максималды ауытқуы 0,5625 болады. Бірінші раундта кілттерді анықтаудың жоғары ықтималдығы $0{,}5625^{16}$ болады, себебі блоктағы 16 S-блоктың барлығы қатысады. Дәл осы сияқты әрбір раунда 16 S-блок қатысып отырғандықтан, екі раундта 32 S-блок, үш раундта 48 S-блок қатысады, сәйкесінше кілтті анықтаудың екі және үш раундтардағы жоғары ықтималдығы $0{,}5625^{32}$ және $0{,}5625^{48}$ болады. Негізінде осындай статистикалық криптоталдаулардың нәтижесі берілген алгоритмнің кірісінен шығысына дейінгі S-блогі ең аз аралықты анықтауға себеп болады. Өйткені алдынала талданған S-блоктің нәтижесі қанша рет кездессе сонша рет еселенеді. Сондықтан біздің қарастырып отырған алгоритміміз үшін сызықтық және дифференциалдық талдауларда әр раундта толық 16 S-блоктың барлығы қатысады.

Егер Мицуру Мацуидің екінші және үшінші леммасына сүйеніп айтатын болсақ [14], әр раундтан кейінгі нәтижелері төмендегідей болады:

Бірінші раундтан кейін алынатын ықтималығы жоғары сызықтық теңдеудің ықтималдығы $\frac{1}{2}+2^{15}\prod_{i=1}^{16}(0{,}5625-0{,}5)=\frac{1}{2}+2^{15}(2^{-4})^{16}=\frac{1}{2}+2^{-49}$ болады, ал кілтті анықтау үшін қалыпты таралу теориясына сәйкес 0,97 ықтималдықпен N = 2^{98} жұп ашық және жабық мәтіндер қажет етеді.

Екінші раундтан кейін алынатын ықтималдығы жоғары сызықтық теңдеудің ықтималдығы $\frac{1}{2}+2^{31}\prod_{i=1}^{32}(0{,}5625-0{,}5)=\frac{1}{2}+2^{31}(2^{-4})^{32}=\frac{1}{2}+2^{-97}$ сәйкес болады, ал кілтті анықтау үшін қалыпты таралу теориясы бойынша 0,97 ықтималдықпен N = 2^{194} жұп ашық және жабық мәтіндер қажет етеді.

Екінші раундтан кейін алынатын ықтималдығы жоғары сызықтық теңдеудің ықтималдығы $\frac{1}{2}+2^{47}\prod_{i=1}^{48}(0{,}5625-0{,}5)=\frac{1}{2}+2^{47}(2^{-4})^{48}=\frac{1}{2}+2^{-145}$ болады, ал кілтті анықтау үшін қалыпты таралу теориясына сәйкес 0,97 ықтималдықпен N=2^{290} жұп ашық және жабық мәтіндер қажет етеді.

Сызықтық талдаудың қортындысы бойынша алгоритмінің беріктілігі үшінші раундтан кейін кілтті толық теруден жоғары екені айқын көрінеді.

*Алгебралық талдау***.** AL04 алгоритміне eXtended Linearization (XL) және eXtended Sparse Linearization (XSL) шабуылдарын қарастырамыз [15-16].

XL шабуылының негізгі идеясы теңдеулер жүйесін барлық полиномдық теңдеулерді сызықтандыру арқылы шешуге тырысу

$$\prod_{l=1}^{k} X_{il}\cdot f_j(X_1,\ldots,X_n)$$

мұндағы, $k \le D-2$.

XL-шабуылы келесідей төрт қадамнан тұрады:

1. Көбейту: $k \le D-2$ үшін $\prod_{l=1}^{k} X_{il}\cdot f_j$ –дің барлық көбейтіндісін алу.

2. Сызықтандыру жүргізу: дәрежесі D-дан кіші немесе тең болатын барлық X_i бірмүшеліктерін тәуелсіз айнымалы ретінде қарастырамыз және 1-қадамда алынған теңдеулерге Гаустың жою әдісін орындаймыз. Барлық мүшелері бір (арнайы)

айнымалыдан тұратындары (мысалы, X_1) ең соңында жойылатындай бірмүшеліктер реттелуі керек.

3. Шешім қабылдау: 2-қадамда кем дегенде X_1 –дің дәрежесі бойынша бірөлшемді бір теңдеу береді деп болжаймыз. Осы теңдеуді ақырлы өрісте шешеміз (мысалы, Berlekamp алгоритмін қолдану арқылы).

4. Қайталау: теңдеулерді қысқартып және басқа айнымалыларды табу үшін осы үрдісті қайталау.

Алдымен берілген S-блокқа қатысты 8 айнымалыдан, 137 мономдардан тұратын 39 квадрат

$$f_1(x_1, \dots, x_8, y_1, \dots, y_8) = 0, \dots, f_{39}(x_1, \dots, x_8, y_1, \dots, y_8) = 0 \quad (5)$$

теңдеулер жүйесін алып, теңдеулерді осы қарастырып отырған GF(2^K) сақинасындағы барлық $\prod_{l=1}^{k} X_{il} \cdot f_j$ мономдарға көбейту арқылы Гаусстың нөлденетін мономдарды қысқартуды пайдалана отырып осы жүйені қайталау арқылы айнымалыларды жеке қалуына дейін қайталаймыз.

Осы қарастырып отырған жүйенің қиындығы төмендегідей жолмен есептеледі. Жалпы теңдеулердің саны алгоритмде қатысатын S-блокдің санына тігелей қатысты $m = r \cdot B \cdot N_r = 39 \cdot 16 \cdot 8 = 4992$.

Айнымалылырдың саны $n = s \cdot B \cdot (N_r - 1) = 8 \cdot 16 \cdot 7 = 896$, мұндағы r - S-блокқа қатысты алынатын квадрат теңдеулер саны, B – бір раундта кездесетін S-блоктар саны, N_r- раунд саны, s - S-блокқа қатысты айнымалылар саны.

$$OS_{XL} = \binom{n}{D}^{\omega} = \binom{896}{21}^{2,376} \approx 2^{325}.$$

XSL әдісі де негізгі төрт кезеңнен тұрады:

1) Алгоритмнің алдағы қадамдарында қолданылатын бірмүшеліктер мен теңдеулердің нақты жиынтығын таңдау арқылы өңделеді.

2) P параметрінің мәнін еркін таңдау және алдыңғы кезеңде таңдалған теңдеулерді $(P-1)$ бірмүшеліктерге көбейту. Бұл XSL шабуылының негізі болып табылады және элементтері алдында таңдалған бірмүшеліктердің көбейтіндісі болатын көп теңдеулер алу керек.

3) Кейбір таңдалған теңдеулерді айнымалыларға көбейтетін T әдісін қолдану. Мұндағы мақсат – жаңа бірмүшеліктер алмай-ақ жаңа теңдеулер құру. Бұл қадам сызықтандыру жүргізу үшін қажетті айнымалылар санымен, жүйеде жеткілікті сызықты тәуелсіз теңдеулер болғанға дейін орындалады.

4) Әрбір бірмүшелікті жаңа айнымалы ретінде қарастыра отырып сызықтандыру жүргізу және Гаусс әдісін қолдану нәтижесінде теңдеулер жүйесінің шешімі алынуы керек.

r теңдеулері мен t мүшелері бар шифрдың әрбір S-блогы үшін бастапқы теңдеулерден бастап, шифрдың құпия кілтін толығымен анықтайтын квадраттық теңдеулер жүйесін құрамыз.

Жоғарыда айтылғандай, XL алгоритмінде дәрежесі (D-2)-ден аспайтын барлық мүмкін болатын бірмүшеліктер, жүйедегі әрбір теңдеуге көбейтіледі. XSL әдісінде оның орнына теңдеулер жүйесі тек таңдалған бірмүшеліктерге көбейту жоспарланады және басқа теңдеулерде пайда болған бірмүшеліктерді көбейту қолданған жөн. $R \geq T$ үшін теңдеулер саны бірмүшеліктер санымен сәйкес келеді және әрбір мүшесіне жаңа айнымалы қосу арқылы теңдеулер жүйесі шешіледі деп күтіледі.

AL04 алгоритмі үшін XSL шабуылдың қиындығы төмендегідей есептеледі,

$$WF \approx \left(\frac{t}{s}\right)^{\omega\left[\frac{t}{r}\right]} \cdot (B \cdot s \cdot N_r^2)^{\omega\left[\frac{t}{r}\right]} = \left(\frac{137}{8}\right)^{2{,}376 \cdot \left[\frac{187}{89}\right]} \cdot (16 \cdot 8 \cdot 8^2)^{2{,}376 \cdot \left[\frac{187}{89}\right]} \approx 2^{261},$$

мұндағы t - S-блокқа қатысты алынатын мономдардың саны, r - S-блокқа қатысты алынатын квадрат теңдеулер саны, B – бір раундта кездесетін S-блоктар саны, N_r- раунд саны, s - S-блокқа қатысты айнымалылар саны, ω – Гаусстың редукция коэффиценті.

Толық алгорим үшін 15344 мономдардан тұратын 4992 теңдеулер жүйесін аламыз. Алгебралық талдау бойынша жүргізілген XL және XSL шабуылдарының қиындығы сәйкесінше 2^{325} және 2^{261} болады.

Талқылау.

Жасалған алгоритм белгілі криптоталдау әдістерін қолдану арқылы сенімділікке тексерілді. Параметрлердің оларға қойылатын талаптарға сай екендігі көрсетілді.

Сондай-ақ құрастырылған шифрлау алгоритмінің сызықтық және дифференциалды криптоталдау үшін қажетті тұрақтылық деңгейін қамтамасыз ететіні анықталды. Алгоритмнің басқа криптографиялық шабуылдарға қарсы беріктігін тексеру үшін зерттеулер жалғасуда.

Жасалған жаңа AL04 шифрлау алгоритмі компьютерлік бағдарлама түрінде жүзеге асырылды, осы бағдарлама негізінде алгоритмнің сенімділігіне зерттеу жүргізілді.

Бағалау нәтижелеріне сүйене отырып, келесі қорытындыларды жасауға болады:

- AL04 шифрлау алгоритмі сызықтық және дифференциалды криптоталдауға қарсылықтың қажетті деңгейін қамтамасыз етеді;
- толық алгоритмнің сызықтық криптоталдау натижелеріне сүйене отырып криптоталдаудың осы түріне қарсы қауіпсіздіктің жоғары деңгейін көрсетті;
- алгебралық криптоталдау нәтижелері алгоритмнің криптографиялық қасиеттерге тән екені анықтады.

AL04 шифрлау алгоритмі радиобайланысты қорғауға бейімделіп құрылған. Ол криптографиялық қорғаудың қажетті деңгейін қамтамасыз етеді және ақпараттық қауіпсіздік талаптарына жауап береді. Криптографиялық қасиеттерді бағалау нәтижелері AL04 алгоритмінің әртүрлі криптоталдау әдістеріне жоғары төзімділігін көрсетеді.

Ұсынылған жұмыстың басты ерекшелігі – зерттеу жұмысы қауіпсіздік бойынша сынақтан өткен отандық әзірлемелер негізінде жүргізілді.

Алынған зерттеу нәтижелерін қолдану қысқа толқынды (КВ) арналар арқылы берілетін құпия ақпаратты қажетсіз және рұқсатсыз ашудан қорғауға мүмкіндік береді.

Алгоритмде матрицаны векторға көбейту амалы орындалатын болғандықтан, бір раундта 16 рет көбейту, ал толық бір блок үшін 128 рет орындалады. Көбейткіштердің біреуі тұрақты болғандықтан, тек қосындылар ретінде қарастыру арқылы алгоритмның жылдамдығын арттыруға болады.

Қорытынды.

Авторлар симметриялы блокты шифрлаудың жаңа алгоритмін жасады, оның құрылымы келесідей түрлендірулерді, сызықты емес түрлендіру ретінде алмастыру кестелерін, көбейту функциясы және раундтық кілттерді қосу амалдардын қамтиды. Әзірленген алгоритмнің артықшылығы – оны қысқа толқынды арна арқылы берілетін ақпаратты шифрлау және шифрды ашу операцияларын орындауға арналған мамандандырылған құрылғыларда тиімді іске асыру мүмкіндігінде. Теориялық және эксперименттік сынақтар алгоритмнің негізгі криптографиялық талаптарға толық сәйкес

келетіндігін көрсетті. Шифрлау алгоритмінің криптотөзімділігін басқа әдістермен зерттеу кейінгі жұмыстарда жалғасатын болады.

Қаржыландыру. Ғылыми-зерттеу жұмысы AP14870419 «ҚТ радиобайланыс бойынша келіссөздерді қорғауға арналған ақпаратты криптографиялық қорғау құралдарын әзірлеу» ҚР БҒМ ҒК гранттық қаржыландыру жобасы аясында жүргізілді.

ӘДЕБИЕТТЕР

[1] Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

[2] Haitner, I., Vadhan, S. (2017). The Many Entropies in One-Way Functions. In: Lindell, Y. (eds) Tutorials on the Foundations of Cryptography. Information Security and Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-319-57048-8_4 [Accessed: 23.02.2024]

[3] Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.

[4] Zhang, W., Cao, M., Guo, J., & Pasalic, E. Improved Security Evaluation of SPN Block Ciphers and its Applications in the Single-key Attack on SKINNY. IACR Transactions on Symmetric Cryptology, 2019, vol. 4, pp. 171–191. https://doi.org/10.13154/tosc.v2019.i4.171-191 [Accessed: 17.02.2024]

[5] Бондаренко А., Маршалко Г., Шишкин В. ГОСТ Р 34.12–2015: чего ожидать от нового стандарта? // Information Security/ Информационная безопасность. – 2015. - №4. – С. 48-50.

[6] Hongru W., Yifan Z. Impossible Differential Cryptanalysis and Linear Cryptanalysis for Eight-Sided Fortress Algorithm. Journal of Electronics & Information Technology, 2023, vol.45(3), pp. 793-799. doi: 10.11999/JEIT221092 [Accessed: 20.02.2024]

[7] Algazy K.T., Babenko L.K., Biyashev R.G., Ishchukova E.A., Kapalova N.A., Nysynbaeva S.E., Andrzej S. Differential Cryptanalysis of New Qamal Encryption Algorithm. International journal of electronics and telecommunications, 2020, vol. 4, pp. 647-653

[8] Liu, F., Isobe, T., Meier, W. MILP-Based Differential Attack on Round-Reduced GIFT (2019) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11405 LNCS, pp. 372-390. doi: 10.1007/978-3-030-12612-4_19 [Accessed: 17.02.2024]

[9] Sze L.Y., Duc-Phong L., Khoongming K. Improved algebraic attacks on lightweight block ciphers. Journal of Cryptographic Engineering 2021, vol. 11, pp.1-9, doi:10.1007/s13389-020-00237-4 [Accessed: 25.01.2024]

[10] Kapalova N, Nyssanbayeva S., Varennikov A., Dyusenbayev D., Sakan K. Higher professional and postgraduate training of information security specialists. Global Journal of Engineering Education, Australia, 2022. V.24, No.3, pp. 232–238. Available at: http://wiete.com.au/journals/GJEE/Publish/vol24no3/10-Sakan-K.pdf. [Accessed: 13.01.2024]

[11] Алгазы К.Т., Капалова Н.А., Сакан К.С., Хомпыш А. Модификация алгоритма шифрования «AL01» // АЭБУ Хабаршысы №1, 2022, - стр.162-170.

[12] Отчет о научно-исследовательской работе «Разработка системы управления криптографическими ключами». - 2020 г. - № гос. регистрации 0118РК000117.

[13] Biham E., ShamirA. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 1991, vol. 4, pp. 3–72.

[14] Matsui, M Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology - EUROCRYPT ’93. 1993, pp. 386–397

[15] Nicolas T., Courtois, Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in Cryptology - ASIACRYPT 2002, pp. 267-287.

[16] Courtois N., Goubin L., Meier W, Tacier J. Solving Underdefined Systems of Multivariate Quadratic Equations. PKC 2002, Springer, pp. 211-227. doi: 10.1007/3-540-45664-3_15

REFERENCES*

[1] Babenko L.K., Ishhukova E.A. Sovremennye algoritmy blochnogo shifrovanija i metody ih analiza. – M.: Gelios ARV, 2006. – 376 s.

[2] Haitner, I., Vadhan, S. (2017). The Many Entropies in One-Way Functions. In: Lindell, Y. (eds) Tutorials on the Foundations of Cryptography. Information Security and Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-319-57048-8_4 [Accessed: 23.02.2024]

[3] Panasenko S.P. Algoritmy shifrovanija. Special'nyj spravochnik. – SPb.: BHV-Peterburg, 2009. – 576 s.

[4] Zhang, W., Cao, M., Guo, J., & Pasalic, E. Improved Security Evaluation of SPN Block Ciphers and its Applications in the Single-key Attack on SKINNY. IACR Transactions on Symmetric Cryptology, 2019, vol. 4, pp. 171–191. https://doi.org/10.13154/tosc.v2019.i4.171-191 [Accessed: 17.02.2024]

[5] Bondarenko A., Marshalko G., Shishkin V. GOST R 34.12–2015: chego ozhidat' ot novogo standarta? // Information Security/ Informacionnaja bezopasnost'. – 2015. - №4. – S. 48-50.

[6] Hongru W., Yifan Z. Impossible Differential Cryptanalysis and Linear Cryptanalysis for Eight-Sided Fortress Algorithm. Journal of Electronics & Information Technology, 2023, vol.45(3), pp. 793-799. doi: 10.11999/JEIT221092 [Accessed: 20.02.2024]

[7] Algazy K.T., Babenko L.K., Biyashev R.G., Ishchukova E.A., Kapalova N.A., Nysynbaeva S.E., Andrzej S. Differential Cryptanalysis of New Qamal Encryption Algorithm. International journal of electronics and telecommunications, 2020, vol. 4, pp. 647-653

[8] Liu, F., Isobe, T., Meier, W. MILP-Based Differential Attack on Round-Reduced GIFT (2019) Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11405 LNCS, pp. 372-390. doi: 10.1007/978-3-030-12612-4_19 [Accessed: 17.02.2024]

[9] Sze L.Y., Duc-Phong L., Khoongming K. Improved algebraic attacks on lightweight block ciphers. Journal of Cryptographic Engineering 2021, vol. 11, pp.1-9, doi:10.1007/s13389-020-00237-4 [Accessed: 25.01.2024]

[10] Kapalova N, Nyssanbayeva S., Varennikov A., Dyusenbayev D., Sakan K. Higher professional and postgraduate training of information security specialists. Global Journal of Engineering Education, Australia, 2022. V.24, No.3, pp. 232–238. Available at: http://wiete.com.au/journals/GJEE/Publish/vol24no3/10-Sakan-K.pdf. [Accessed: 13.01.2024]

[11] Algazy K.T., Kapalova N.A., Sakan K.S., Hompysh A. Modifikacija algoritma shifrovanija «AL01» // AJeBU Habarshysy №1, 2022, - str.162-170.

[12] Otchet o nauchno-issledovatel'skoj rabote «Razrabotka sistemy upravlenija kriptograficheskimi kljuchami». - 2020 g. - № gos. registracii 0118RK000117.

[13] Biham E., ShamirA. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 1991, vol. 4, pp. 3–72.

[14] Matsui, M Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology - EUROCRYPT ’93. 1993, pp. 386–397

[15] Nicolas T., Courtois, Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in Cryptology - ASIACRYPT 2002, pp. 267-287.

[16] Courtois N., Goubin L., Meier W, Tacier J. Solving Underdefined Systems of Multivariate Quadratic Equations. PKC 2002, Springer, pp. 211-227. doi: 10.1007/3-540-45664-3_15

Nursulu Kapalova, candidate of technical sciences, associate professor, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, nkapalova@mail.ru

Saule Nyssanbaeva, doctor of technical sciences, associate professor, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, Sultasha1@mail.ru

Dilmukhanbet Dyusenbayev, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, dimash_dds@mail.ru

Ardabek Khompysh, PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, ardabek@mail.ru

DEVELOPMENT OF THE AL04 ENCRYPTION ALGORITHM AND STUDY OF ITS CRYPTOGRAPHIC PROPERTIES

Abstract. Negotiations conducted via any means of radio communication cannot be confidential by their nature, as they can be intercepted by interested parties. As ensuring the security of radio communications remains a relevant issue, the enhancement of radio communication systems with a cryptographic information protection module is proposed. This module will be functionally housed in a separate enclosure and inserted into the gap between the radio station and the handset. The developed cryptographic information protection tools are entirely domestically produced. The information encryption algorithm and schematic solutions comply with the requirements of information security and are "transparent" for certification according to the state standard ST RK 1073-2007. A new encryption algorithm AL04 has been developed for the information protection module. This paper provides a description of this algorithm and the results of evaluating its cryptographic properties. The main parameters of AL04 are as follows: block length - 128 bits; key length - 128 bits; number of rounds - 8. Additionally, the results of evaluating the resistance of the developed encryption algorithm to various cryptanalysis methods have been obtained.

In particular, it has been demonstrated that the developed encryption algorithm provides the necessary level of resistance to linear and differential cryptanalysis. Furthermore, a linear cryptanalysis of the entire algorithm was conducted, and the AL04 encryption algorithm showed a high level of security against this type of cryptanalysis. The AL04 encryption algorithm was also subjected to algebraic cryptanalysis. The research results indicate that this algorithm exhibits strong cryptographic properties.

Keywords. Cryptographic strength, differential cryptanalysis, linear cryptanalysis, algebraic cryptanalysis.

Нурсулу Капалова, к.т.н., ассоциированный профессор, Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан, nkapalova@mail.ru

Сауле Нысанбаева, д.т.н., доцент, Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан, Sultasha1@mail.ru

Дилмуханбет Дюсенбаев, Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан, dimash_dds@mail.ru

Ардабек Хомпыш, PhD, Институт информационных и вычислительных технологий КН МНВО РК, Алматы, Казахстан, ardabek@mail.ru

РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ AL04 И ИССЛЕДОВАНИЕ ЕГО КРИПТОГРАФИЧЕСКИХ СВОЙСТВ

Аннотация. Переговоры, осуществляемые по любым средствам радиосвязи, не могут быть конфиденциальными по своей природе, так как возможен их перехват заинтересованными лицами. Так как защита радиопереговоров является актуальным вопросом, то в качестве решения предложено дооснащение системы радиосвязи модулем криптографической защиты информации, который функционально будет размещаться в отдельном корпусе и включаться в разрыв между радиостанцией и тангентой. Разрабатываемые средства криптографической защиты информации являются полностью отечественным продуктом. Алгоритм шифрования информации и схемные решения отвечают требованиям информационной безопасности и «прозрачны» для сертификации по государственному стандарту СТ РК 1073-2007. Для модуля защиты информации разработан новый алгоритм шифрования AL04. В данной работе приводится описание этого алгоритма и результаты оценки его криптографических свойств. Основные параметры AL04: длина блока – 128 бит; длина ключа – 128 бит; количество раундов – 8. Также получены результаты оценки стойкости разработанного алгоритма шифрования к различным методам криптоанализа.

В частности, было продемонстрировано, что разработанный алгоритм шифрования обеспечивает необходимый уровень устойчивости к линейному и дифференциальному криптоанализу. Кроме того, был проведен линейный криптоанализ полного алгоритма, и алгоритм шифрования AL04 показал высокий уровень безопасности против этого типа криптоанализа. Алгоритм шифрования AL04 также был подвергнут алгебраическому криптоанализу. Результаты исследования показывают, что этот алгоритм демонстрирует сильные криптографические свойства.

Ключевые слова. Криптографическая стойкость, дифференциальный криптоанализ, линейный криптоанализ, алгебраический криптоанализ**.**

****

Келіп түсті: 12 сәуір 2024 ж.; қабылданды: 25 тамыз 2024 ж.