3. Ганиев С.К., Халмуратов О.У., Худайкулов З., «Detection weighty coefficient of functional requirements classes of standard “information technology. security techniques evaluation criteria for it security”, «Химическая технология. Контроль и управление», Ташкент, 2014, №2.

Халмуратов Омонбой Утамуратович

Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Урганч филиали Ахборот технологиялари кафедраси мудири.
Тел:+998901186425
Эл почта: omonboyx@gmail.com

УДК 681.3

Khalmuratov O.U.

Functional model of system of criteria and indicators of information security

This article is devoted to the formation of information security criteria and indicators and the development of the functional model of the organization's information security assessment n the basis of IDEF 0 methodology.

Keywords: IDEF 0 Methodology, Information security criteria and indicators, fuzzy logic theory, fuzzy sets theory, methods of assessment, information security assessment..

Д. Е. Акбаров, Э. К. Мадаминов, Ш.А. Умаров

СИММЕТРИК БЛОКЛИ ШИФРЛАШ АЛГОРИТМЛАРИ КРИПТОБАРДОШЛИЛИК МЕЗОНЛАРИНИ – КРИТЕРИЙЛАРИНИ ТЕКШИРИШ ВОСИТАЛАРИ

Мақолада симметрик блокли шифрлаш алгоритмларига қўйиладиган криптобардошликнинг зарурийлик шартларини ёки критерийларини текширишнинг воситалари асосларини: математик модел, умумий қоида, таъмоил, тавсиялар ифодасида ишлаб чиқиш масаласи ечими таҳлил этилган.

Таянч сўзлар: симметрик блокли шифрлаш, криптобардошлик критерийлари, базавий акслантиришлар. чизиқсизлик, мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш, корреляцияга мосланувчанлик, Фестел тармоғи.

Кириш. Ўрнига қўйиш шифрлаш алгоритмларидан фойдаланишда очиқ маълумот частотавий хусусиятларининг шифрмаълумотга кўчмаслигини таъминлаш учун кўп алифболи шифрлаш алгоритмларидан фойдаланилади, бунга эришиш учун эса, шифрлаш жараёни босқичларида бир хил белгиларни ҳар хил белгиларга алмаштириш, яъни калит узунлигини ошириш зарурияти туғилади [1-4].

Мутлақо бардошли ва узликсиз шифрлаш алгоритмлари кўп алифболи бўлиб, криптобардошли ҳамда аппарат қурилмаларини ишлаб чиқилиши қулай. Аммо улар шифрлаш калитининг бир марта қўлланилиши ва унинг узунлигини катта ҳажмга эгалиги, унинг муҳофазасини кафолатли таъминланган ҳолда сақлашда ва тегишли фойдаланувчиларга етказишни амалга оширишда хотира ҳамда ахборот-коммуникация тармоғида узатишда кўп вақт талаб этиши каби ноқулайликларни келтириб чиқаради. Бундай ноқулайликларни бартараф этишдаги илмий изланишлар симметрик блокли шифрлаш алгоритмлари яратилиши заруриятини келтириб чиқарди.

Симметрик блокли шифрлашда очиқ маълумотни уни ташкил этувчи алиффбо белгиларининг маълум бир узунликдаги бирикмалари (блоклари) бирлашмаси (конкатенацияси) кўринишда ифодалаб, ана шу блокларнинг алоҳида-алоҳида самарали ва криптобардошли шифрланишини таъминлаш амалга оширилади. Симметрик блокли шифрлаш алгоритмларининг асосини очиқ маълумот блокларини юқори даражада *аралаштириш* ва *тарқатиш* хоссаларига эга бўлган акслантиришлар ташкил этади [5-7]. Бардошли криптоалгоритмлар туркумига кирувчи симметрик блокли шифрлаш алгоритмлари асосидаги акслантиришларнинг ечилиши мураккаб бўлган математик масалалар билан боғлиқлик хусиятлари чуқур таҳлил қилинмаган бўлсада, бу акслантиришлар криптобардошлигини самарали тезкор амалга ошириш имкониятлари қулайдир [3,4].

Масаланинг қўйилиши. Симметрик блокли шифрлаш алгоритмлари криптобардошлигининг зарурийлик критерийларини текшириш воситалари асосларини ишлаб чиқиш муҳим масалалардан ҳисобланади [4].

Масланинг ечилиши. Фан-техника ва технологиялари ютуқларидан фойдаланиб, барча мумкин бўлган калитларни танлаб олишда ҳисоблаш ресурслари ҳаражати ҳамда вақт сарфини таъминловчи калит узунлигининг қуйи чегараси – кафолатланган калит узунлиги ҳисобланади [1-5].

Фестел тармоқли симметрик блокли шифрлаш алгоритмлари акслантиришларининг умумий хусусиятлари ва криптобардошлигига қўйиладиган критерийлар қуйидагилардан иборат [4]:

1) Алгоритмнинг криптобардошлиги унинг маҳфий сақланишига боғлиқ бўлмай, фақат

калитнинг маҳфий тутилишига ва узунлигига боғлиқ. Унинг узунлиги калитни ташкил этувчи белгиларнинг қандай ишлатилишига кўра калит алфавитидан аниқланади. Бунда калитни ташкил этувчи алфавит белгилари сони 128 тадан кам эмас: $k = k_1 k_2 ... k_N, \quad k_i \in \{0;1\}, N = 32 \times l, \quad l = 4,5,\ldots < \infty;$

2) Акслантирилувчи блок узунлиги $2^t, \quad t = 6,7,\ldots < \infty$ бўлиши, алгоритм акслантиришларида қўлланиладиган амаллар микропроцессор, микроконтроллер ва ҳисоблаш технологиялари имкониятларидан самарали фойдаланишга мос бўлиши лозим;

3) Асосий акслантиришларининг самарали аралаштириш ва тарқатиш хусусиятига эгалиги таъминланган бўлиши керак;

4) Базавий акслантиришлари чизиқсизлик, мувозанатлашганлик, регулярлик, корреляцияга мосланувчанлик каби хоссаларга эга бўлиши лозим;

5) Базавий акслантиришларининг биртомонламали бўлишига эришиш зарур.

Криптобардошлик зарурийлик мезонлари таснифлари бу шартлар бузилганда криптобардошликка салбий таъсир этувчи ҳолатларни келиб чиқиши билан асосланган [4].

1. Биринчи критерий алгоритм криптобардошлигига шубҳа бўлмаслигини таъминлаш чора ва тадбирлари масалаларини ечимлари билан боғлиқ бўлиб, Кирхгофс тамойилига роя қилинганлигини ва кафолатланган калит узунлигини билдиради.

Алгоритмнинг маълум бўлмаслиги, ундан фойдаланувчиларда криптобардошлигига шубҳа туғдиради, бу эса унинг кенг миқиёсда қўлланилишини чеклайди. Калит алфавитига кўра шифрлаш калити узунлигидаги алфавит белгилари сони 128 тадан кам бўлиши, бугунги кун фан-техника ва технологиялари ютуқларидан фойдаланган ҳолда криптоҳужум турини самарали амалга оширишга қулайлик туғдиради. Шунинг учун калитни ташкил этувчи белгиларнинг қандай ишлатилишига кўра калит алфавити аниқланиб, калитни ташкил этувчи алфавит белгилари сони 128 тадан кам эмаслиги текширилиши лозим.

2. Иккинчи критерий зарурият туғилганда криптабардошликни ошириш учун алгоритм базавий акслантиришларини сақлаб қолган ҳолда калитни узайтириб, уни самарали модификациялаш имкониятини беради [3,4]. Бу эса унинг аппарат қурилмаларини яратилишига қулайлик туғдиради ва тез ишлашини таъминлайди.

Акслантирилувчи блок узунлиги қиймати иккининг даражалари кўринишида бўлмаслиги, яъни $2^t, \quad t = 6,7,\ldots < \infty$ бўлмаслиги, криптабардошликни ошириш учун зарурият туғилганда унинг аппарат қурилмаларини яратилишига ноқулайлик туғдиради ва тез ишлашини таъминлайдиган базавий акслантиришларини сақлаб қолган ҳолда самарали модификациялаш имкониятини бермайди [3].

3. Учинчи ва тўртинчи критерийлар алгоритм акслантиришларининг криптоҳужумларга бардошли бўлишини таъминлаш учун зарур. Асосий акслантиришларининг самарали аралаштириш ва тарқатиш хусусиятига эга эмаслиги алгоритм акслантиришларининг чизиқли ва дифференциал криптотаҳлил усулларига бардошли бўлмаслигига олиб келади.

Базавий акслантиришлари чизиқсизлик, мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш самарадорлик, корреляцияга мосланувчанлик каби хоссаларга эга бўлмаса, чизиқли, дифференциал ва бошқа криптохужум усулларини қўллаб шифрлаш калитини топиш эҳтимоллиги ортади.

Базавий акслантиришларнинг санаб ўтилган бардошликни таъминловчи хоссаларга эга бўлиши акслантиришнинг жуфт-жуфти билан ҳар хил бўлган барча мумкин бўлган кириш блокларига жуфт-жуфти билан ҳар хил бўлган чиқиш блокларини мос қўйишини, яъни биектив бўлишини текшириш билан амалга оширилади. Ҳақиқатан ҳам, бу тасдиқни тўғрилигини, қулайлик учун кириш ва чиқиш блоклари узунлиги тўртга тенг бўлганда кўриб ўтилади.

Қулайлик учун $n = m = 4$ деб олинди ва ушбу $Y = f(X): GF(2)^4 \to GF(2)^4$ биектив акслантиришнинг ҳамда унга тескари $X = f^{-1}(Y)$: $GF(2)^4 \to GF(2)^4$ акслантиришнинг чинлик жадваллари берилган:

Жад.1.

$x_1\ x_2\ x_3\ x_4$	$f_1\ f_2\ f_3\ f_4$
0 = 0 0 0 0	0 1 0 0 = 4
1 = 0 0 0 1	1 1 1 1 = 15
2 = 0 0 1 0	0 0 1 1 = 3
3 = 0 0 1 1	0 0 0 0 = 0
4 = 0 1 0 0	1 0 0 1 = 9
5 = 0 1 0 1	1 1 0 0 = 12
6 = 0 1 1 0	1 1 0 1 = 13
7 = 0 1 1 1	1 0 1 0 = 10
8 = 1 0 0 0	1 0 0 0 = 8
9 = 1 0 0 1	0 1 1 1 = 7

Жад. 2.

$f_1\ f_2\ f_3\ f_4$	$x_1\ x_2\ x_3\ x_4$
0 = 0 0 0 0	0 0 1 1 = 3
1 = 0 0 0 1	1 1 0 0 =12
2 = 0 0 1 0	1 0 1 1 =11
3 = 0 0 1 1	0 0 1 0 = 2
4 = 0 1 0 0	0 0 0 0 = 0
5 = 0 1 0 1	1 1 1 0 =14
6 = 0 1 1 0	1 0 1 0 =10
7 = 0 1 1 1	1 0 0 1 = 9
8 = 1 0 0 0	1 0 0 0 = 8
9 = 1 0 0 1	0 1 0 0 = 4

10 = 1 0 1 0	0 1 1 0 = 6
11 = 1 0 1 1	0 0 1 0 = 2
12 = 1 1 0 0	0 0 0 1 = 1
13 = 1 1 0 1	1 0 1 1 = 11
14 = 1 1 1 0	0 1 0 1 = 5
15 = 1 1 1 1	1 1 1 0 = 14

10 = 1 0 1 0	0 1 1 1 = 7
11 = 1 0 1 1	1 1 0 1 =13
12 = 1 1 0 0	0 1 0 1 = 5
13 = 1 1 0 1	0 1 1 0 = 6
14 = 1 1 1 0	1 1 1 1 =15
15 = 1 1 1 1	0 0 0 1 = 1

Бу чинлик жадваллари бул функция ифодалари қуйидагича [3]:

а) ушбу $Y = f(X): GF(2)^4 \to GF(2)^4$ бул функция акслантиришлари:

$$f_1 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1x_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (\overline{x}_1x_2x_3x_4) \oplus (x_1\overline{x}_2\overline{x}_3\overline{x}_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3x_4);$$
$$f_2 = (\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2\overline{x}_3x_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus (x_1\overline{x}_2x_3\overline{x}_4) \oplus (x_1x_2x_3\overline{x}_4) \oplus (x_1x_2x_3x_4);$$
$$f_3 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1\overline{x}_2x_3\overline{x}_4) \oplus (\overline{x}_1x_2x_3x_4) \oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus$$
$$\oplus (x_1\overline{x}_2x_3\overline{x}_4) \oplus (x_1\overline{x}_2x_3x_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3x_4);$$
$$f_4 = (\overline{x}_1\overline{x}_2\overline{x}_3x_4) \oplus (\overline{x}_1\overline{x}_2x_3\overline{x}_4) \oplus (\overline{x}_1x_2\overline{x}_3\overline{x}_4) \oplus (\overline{x}_1x_2x_3\overline{x}_4) \oplus$$
$$\oplus (x_1\overline{x}_2\overline{x}_3x_4) \oplus (x_1x_2\overline{x}_3\overline{x}_4) \oplus (x_1x_2\overline{x}_3x_4) \oplus (x_1x_2x_3\overline{x}_4);$$

б) ҳамда тескари $X = f^{-1}(Y): GF(2)^4 \to GF(2)^4$ бул функция акслантиришлари:

$$x_1 = (\overline{f}_1\overline{f}_2\overline{f}_3f_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1f_2\overline{f}_3f_4) \oplus (\overline{f}_1f_2f_3\overline{f}_4) \oplus$$
$$\oplus \overline{f}_1f_2f_3f_4) \oplus (f_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (f_1f_2\overline{f}_3f_4) \oplus (f_1f_2f_3\overline{f_4});$$
$$x_2 = (\overline{f}_1\overline{f}_2\overline{f}_3f_4) \oplus (\overline{f}_1f_2\overline{f}_3f_4) \oplus (f_1\overline{f_2}\overline{f}_3f_4) \oplus (f_1\overline{f_2}f_3\overline{f}_4) \oplus$$
$$\oplus (f_1\overline{f}_2f_3f_4) \oplus (f_1f_2\overline{f_3}\overline{f}_4) \oplus (f_1f_2\overline{f_3}f_4) \oplus (f_1f_2f_3\overline{f_4});$$
$$x_3 = (\overline{f}_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1\overline{f_2}f_3f_4) \oplus (\overline{f}_1f_2\overline{f_3}f_4) \oplus$$
$$\oplus (\overline{f_1}f_2f_3\overline{f}_4) \oplus (f_1\overline{f}_2f_3\overline{f}_4) \oplus (f_1f_2\overline{f_3}f_4) \oplus (f_1f_2f_3\overline{f_4});$$
$$x_4 = (\overline{f}_1\overline{f}_2\overline{f}_3\overline{f}_4) \oplus (\overline{f}_1\overline{f}_2f_3\overline{f}_4) \oplus (\overline{f}_1f_2f_3f_4) \oplus (f_1\overline{f_2}f_3\overline{f}_4) \oplus$$
$$\oplus (f_1\overline{f}_2f_3f_4) \oplus (f_1f_2\overline{f_3}\overline{f}_4) \oplus (f_1f_2f_3\overline{f}_4) \oplus (f_1f_2f_3f_4).$$

Бу акслантиришлар асосида кетма-кет мумкин бўлган ушбу

$$(0)_{10} = (0000)_2 \le x = (x_1, x_2, x_3, x_4) \le (1111)_2 = (15)_{10}$$

кириш блокларида тегишли ҳисоблашларга кўра Жад.1. ва Жад.2. ҳосил қилинади.

Бул функцияларни ҳамда уларга мос Жад.1. ва Жад.2. таҳлил қилиниб, 3-критерий ва 4-критерий шартларини текшириш мумкин.

Чинлик жадвали Жад.1. бўйича барча f_i, $i = 1,2,3,4;$ устунлардаги “0” ва “1” ларни сони тенглиги аниқланади, бундан эса $Y = f(X): GF(2)^4 \to GF(2)^4$ акслантиришнинг мувозанатлашганлиги (регулярлиги ҳам) таърифга кўра келиб чиқади [5].

Шунингдек, чинлик жадваллари таҳлилига кўра $Y = f(X): GF(2)^4 \to GF(2)^4$ акслантиришнинг чиқиш блокларининг ўзгариши кириш блоклари битларининг бирор қонуният билан ўзгаришига боғлиқ эмаслиги кўринади, яъни кириш блоклари битларининг ўзгариши чиқиш блокларининг ўзгариши билан статистик боғлиқ эмас. Бундан акслантиришнинг корреляцияга мосланувчанлик ва қатъий кескин ўзгариш самарадорлик хоссаларини таъминланганлиги таърифга мос равишда ўрнатилади [5].

Жад.1. бўйича аниқланган $Y = f(X): GF(2)^4 \to GF(2)^4$ акслантиришни аниқловчи бул функциялар f_i, $i = 1,2,3;$ ифодаларида $\overline{x}_i = x_i \oplus 1$ алмаштириш қилиниб, тегишли соддалаштиришлардан сўнг фақат x_i –ўзгарувчилардан конъюнкциясидан иборат ҳадларга боғлиқ ифодаларга эга бўлинади.

Ҳадларида x_i –ўзгарувчиларнинг қатнашганлиги сони билан улар чизиқсизлиги даражасини аниқлайди. Кўрилаётган акслантириш мисолида ҳар бир f_i , $i = 1,2,3;$ ифодаларида ушбу ҳад $x_1x_2x_3x_4$ қатнашган, f_4 ифодасида $x_1x_2x_3\overline{x_4}$. Бевосита ҳисоблаш ва соддалаштиришлардан сўнг бу ифодаларнинг чизиқсиз бул функциялар эканлигига ишонч ҳосил қилиш мумкин.

Келтирилган мисолдаги $Y = f(X)$: $GF(2)^4 \to GF(2)^4$ сюректив эканлигидан, юқоридаги статистик боғлиқсизлик ҳамда текис тақсимотлилиги чизиқли ва дифференциал криптоҳужум турларини самарасиз бўлишини таъминлайди.

4. Бешинчи критерий алгоритм акслантиришларига тескари акслантиришлардан фойдаланиб амалга оширилиши мумкин бўлган криптоҳужумларга бардошлиликни таъминлайди.

Базавий акслантиришларининг тегишли изоҳлар билан биртомонламалик хусусиятига эга бўлмаслиги алгоритм акслантиришларига тескари акслантиришлардан фойдаланиб амалга оширилиши мумкин бўлган криптоҳужумларга кенг шароит яратади.

Назарий жиҳатдан ҳар қандай акслантиришнинг чинлик жадвалини тузиш мумкин. Бундай ҳолат эса тескари жадвалли акслантиришнинг мавжуд эканлигини билдиради. Аммо акслантиришларнинг кўп алфавитли бўлиши унга тескари бўлган акслантиришни амалий жиҳатдан мураккаб бўлишини таъминлайди. Симметрик блокли шифрлаш алгоритмлари акслантиришларининг кўп алфавитли бўлиши раундлар ва улар калитлари билан боғлиқ акслантиришлар хусусиятлари орқали таъминланган [3,4].

Олинган натижалар таҳлили. Симметрик блокли шифрлаш алгоритми туркуми учун криптобардошликни зарурийлик мезонлари шартларини текширишга асос бўлувчи математик ёндошув усуллари, модел, тавсия ва воситалар акслантиришларни тегишли мезонлар бўйича таҳлил этишнинг тамойилларини белгилайди.

Акслантиришларни тегишли мезонлар бўйича таҳлил этишнинг тамойиллари фан-техника ва технологияларнинг ютуқларига, янги асосли алгоритмлар яратилиши каби жараёнларга боғлиқ ҳолада тизимли равишда бойитиб борилади.

Хулоса. Олинган натижалар симметрик блокли шифрлаш туркумдаги алгоритмлар бардошлиги зарурийлик мезонлари шартларини амалда текширишда илмий қўлланма учун асос бўла олади.

Адабиётлар:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд.–М.: Гелиос АРВ, 2002.-480 с.

3. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, «Ўзбекистон маркаси», 2009 – 434 бет.

4. Акбаров Д.Е., Мухтаров Ф.М., Сиддиқов А.А. Криптотахлил масалаларига тизимли ёндошув асослари ва уларни ечиш усуллари. – Фарғона. “ФАРҒОНА”» нашрёти, 2014 й. –143 бет.

5. Акбаров Д.Е., Умаров Ш.А. Разработка нового алгоритма шифрования данных с симметричным ключом // Journal of Siberian Federal University. Engineering & Technologies, 2016, 9(2), 214-224

6. Акбаров Д.Е., Умаров Ш.А., Хасанов Х. М. Ахборот муҳофазасини таъминлаш воситаларининг баъзи масалалари ечимларига мантиқий амаллар тадбиқи. стр. // ФарПИ Илмий-техника журнали. -2016, том № 20, махсус нашр. –29-33 бетлар.

7. Молдовян Н. А., Молдовян А. А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

1. Акбаров Давлатали Егиталиевич – доктор физико-математических наук.
Кокандский государственный педагогический институт.
E-mail: bardosh9295@mail.ru

2. Мадаминов Эркин Комилович – инженер.
Кокандский государственный педагогический институт.
E-mail: bardosh9295@mail.ru

3. Умаров Шухратжон Азизжонович – старший преподаватель.
Ферганский филиал Ташкентского университета информационных технологий.
E-mail: sht00357@gmail.com

D.E.Akbarov, E. K.Madaminov , Sh.A.Umarov

Means of checking necessary conditions - criterion of crypto stability of symmetric block encryption algorithm

The article investigates the solution of the problem to develop the foundations of means for checking necessary conditions or the criterion for cryptographic stability of symmetric block encryption algorithms in the form of: mathematical models, general rules, principles, recommendations, etc.

Keywords: *symmetric block ciphering, criterion of cryptostability, basic transformations, nonlinearity, balance, regularity, severe avalanche effect, correlation immunity, Feistelian networks.*