Таблица 2

Вариация, нТл	<5	5-10	10-20	20-40	40-70	70-120	120-200	200-330	330-550	>550
К-индекс	0	1	2	3	4	5	6	7	8	9
Интерпретация	Спокойное		Слабо-возмущенное		Возму-щенное	Магнитная буря		Большая магнитная буря		

Преимуществами предлагаемого подхода прогнозирования является отсутствие процедур экстраполяции, т.е. точность прогноза индексов ГМА не зависит от срока прогнозирования.

Литературы:

1. Огурцов М.Г.: 2005. Современные достижения солнечной палеоастрофизики и проблемы долговременного прогноза активности Солнца. Астрономический Журнал. Т. 82, № 6,
2. Амиантов А. С., Зайцев А. Н., Одинцов В. И., Петров В. Г. Вариации магнитного поля Земли. М., 2001.
3. Константиновская Л.В. Положение планет и долгосрочное прогнозирование. — Математические методы анализа цикличности в геологии, вып.6, РАЕН, М., 1994, с.113-117.
4. Герасимов И.А., Мушаилов Б.Р., Копаев А.В. Динамическое воздействие больших планет на характеристики солнечного цикла. Труды конференции "Астрометрия, геодинамика и небесная механика на пороге XXI века". СПб: ИПА РАН. 2000. С. 265 - 266.
С. 555-560.
5. Дубров А.М., Мхитарян В.С., Трошин Л.И. Многомерные статистические методы. М.: Финансы и статисткиа, 2000. - 352 с.
6. Cartwright D., Edden A. Corrected tables of tidal harmonics. J. Geophys. Res. 33, №3, 253-63 (1973).
7. Cartwright D.E., Tayler R.I. New Computations of the Tide-generating Potential. Geophys. J. Roy. Astron. Soc., 23, 45-47 (1971)
8. http://www.ijarset.com/volume-4-issue-10-october-2017.html

УДК 681.3

Д. Е. Акбаров, У. Б. Бекмуродов, Э. К. Мадаминов, Ш. А. Умаров

УЗЛУКСИЗ ШИФРЛАШ АЛГОРИТМЛАРИ КРИПТОБАРДОШЛИЛИК МЕЗОНЛАРИНИ – КРИТЕРИЙЛАРИНИ ТЕКШИРИШ

Ушбу мақолада узликсиз шифрлаш алгоритмлари криптобардошлигини зарурийлик мезонларини-критерийларини текширишнинг илмий асосланган воситалари моделларини ишлаб чиқиш ва амалий тадбиқларини амалга ошириш каби масалалар таҳлил этилиб, уларнинг ечимлари асосий тамоиллари ёритилади.

Таянч сўзлар: узликсиз шифрлаш, криптобардошлик критерийлари, базавий акслантиришлар. чизиқсизлик, регулярлик, мувозанатлашганлик, қатъий кескин ўзгариш, корреляцияга мосланувчанлик, псевдотасодифий кетма-кетлик, биртомонламалик.

Кириш. *Мутлақо бардошли* криптоалгоритмлар ишончли бўлсада амалий татбиқда ноқулайликлар ҳам мавжуд. Хусусан, шифрлаш калитининг бир марта қўлланилишидан келиб чиқадиган катта ҳажмдаги узунликка эга бўлишлик хоссасига кўра унинг муҳофазасини кафолатли таъминланган ҳолда сақлаш ва тегишли фойдаланувчиларга етказишни амалга оширишдир. Шу каби ноқулайликларни бартараф этиш зарурияти асосида узлуксиз шифрлаш алгоритмлари яратилиши табиий равишда вужудга келган.

Нисбатан кичик узунликка эга бўлган, яъни кафолатланган криптобардошлиликни таъминловчи узунликка эга бўлган – бугунги кунда 128 битдан кам бўлмаган калит билан бир томонлама криптографик акслантиришлар асосида, етарли даражада катта узунликдаги псевдотасодифий кетма-кетлик (ПТКК) гаммасини ишлаб чиқарувчи генераторлар негизида узлуксиз шифрлаш алгоритмлари яратилади [1-4].

Криптабардошлиги калит узунлиги ва акслантиришлари биртомонламалик хусусиятли, масалан: байтлар ўрнини боғлиқсиз алмаштириш, сиқиш жадвали, иккита сатри ёки устуни мос элементлари пропорционал бўлган матрицали кенгайтириш, чинлик жадвали тенг тақсимот хусусиятига эга бўлган мантиқий функциялар, псевдо-тасодифий кетма-кетлик (ПТКК) ишлаб чиқарувчи генераторлар моделларини комбинациялаш каби тизимлардан иборат.

Масаланинг қўйилиши. Ушбу мақолада зарурийлик мезонларини текширишнинг илмий асосланган воситалари моделларини ишлаб чиқиш ва

амалий тадбиқларини амалга ошириш каби масалалар таҳлил этилиб, уларнинг ечимлари асосий тамоиллари ёритилади.

Масаланинг ечилиши. Узликсиз шифрлаш алгоритмларига қўйиладиган зарурийлик шартлар ёки критерийлар [3,4]:

1) Алгоритм очиқ (маълум) бўлиб, унинг криптобардошлиги алгоритмни маҳфий сақланишига боғлиқ бўлмай фақат калитнинг маҳфий тутилишига ва узунлигига боғлиқ, унинг узунлиги 128 битдан кам эмас:

$$k = k_1 k_2 ... k_N, \quad k_i \in \{0;1\}, N = 32 \times l, \quad l = 4,5,... < \infty$$

2) Алгоритм акслантиришларида қўлланиладиган амаллар микропроцессор, микроконтроллер ва компьютер ҳисоблаш технологиялари имкониятларидан самарали фойдаланишга мос бўлиши лозим;

3) Асосий акслантиришларининг самарали аралаштириш ва тарқатиш хусусиятига эгалиги таъминланган: акслантиришлари чизиқсизлик, мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш самарадорлик, корреляцияга мосланувчанлик каби хоссаларга эга бўлиши лозим;

4) Асосий акслантиришлари биртомонламалик хусусиятига эга;

5) Алгоритм етарли узун даврга эга бўлган кетма-кетлик ишлаб чиқишни таъминлаши керак;

6) Ишлаб чиқилган ПТКК блокининг бир битдан, икки битдан, уч битдан, ярим байт ва ҳокозо қисм блокларидан иборат кетма-кетлиги текис статистик тақсимот кўрсаткичига эга бўлиши керак;

7) Псевдотасодифий кетма-кетликнинг гамма элементлари (бит, ярим байт, байт, қисм блоклари) барча бошқа элементларининг ҳиссаси орқали ҳосил қилиниши (силжитиш регистрлари асосида ишлаб чиқариладиган тасодифий кетма-кетлик каби) ─ аралашиш самарали бўлиши керак.

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

1. Критерий 1) алгоритм криптобардошлигига шубҳа бўлмаслигини таъминлаш масалаларини ечимлари билан боғлиқ бўлиб, Кирхгофс таъмоилига роя этилганлигини ва кафолатланган калит узунлигини аниқланганлигини билдиради.

Алгоритмнинг очиқ (маълум) бўлмаслиги, ундан фойдаланувчиларда криптобардошлигига шубҳа туғдиради, бу эса унинг кенг миқиёсда қўлланилишини чеклайди.

Узликсиз шифрлаш туркумидаги алгоритмлар содда ва тез ҳисоблашларни амалга оширувчи акслантиришлардан иборат эканлигини инобатга олинса, калити узунлигининг 128 битдан кам бўлиши бугунги кун фан-техника ва технологиялари ютуқларидан фойдаланган ҳолда мумкин бўлган барча калитларни танлаб чиқиш криптоҳужум турини самарали амалга оширишга қулайлик туғдиради.

Калит алфавити белгиларининг шифрлаш алгоритми акслантиришларида калитни ташкил этувчи белгиларнинг қандай ишлатилиши билан аниқланади, масалан:

– агар акслантиришлар битлар устида амалга ошириладиган бўлса, маҳфий калит алфавити битлардан иборат бўлиб, 128 битдан кам бўлмаслиги лозим;

– агар акслантиришлар ярим байтлар ёки байтлар устида амалга ошириладиган бўлса, маҳфий калит алфавити мос равишда ярим байт ёки байтлардан иборат бўлиб, 128 ярим байт ёки байтдан кам бўлмаслиги каби шартлар муҳимдир.

Калитни ташкил этувчи белгиларнинг қандай ишлатилишига кўра калит алфавити аниқланиб, калитни ташкил этувчи алфавит белгилари сони 128 тадан кам эмаслиги текширилиши лозим.

2. Критерий 2) алгоритмнинг аппарат қурилмаларини яратилишига қулайлик туғдиради ва тез ишлашини таъминлашга асос бўлади.

Алгоритм акслантиришларида қўлланиладиган амаллар микропроцессор, микроконтроллер ва компьютер ҳисоблаш технологиялари имкониятларидан самарали фойдаланишга мос бўлмаса унинг аппарат қурилмаларини яратилишига қулайлик туғдирмайди ва тез ишлашини таъминламайди;

Акслантиришларда қўлланиладиган амалларнинг чинлик жадвали элементлари тенг тақсимланган битлар устида бажариладиган мантиқий ёки ярим байт ҳамда байтлар каби жадвалли алмаштиришлардан иборат бўлиши мақсадга мувофиқ [5].

3. Критерий 3) алгоритм акслантиришларининг криптоҳужумларга бардошли бўлишини таъминлаш учун зарур.

Битлар бирикмалари билан боғлиқ амаллар бажариладиган асосий акслантиришларга эга бўлинса, уларнинг самарали аралаштириш ва тарқатиш хусусиятига эгалигини таъминланмагани уларга нисбатан криптоҳужумларни самарали амалга оширилишини келтириб чиқаради:

– бундай акслантиришларнинг самарали аралаштириш ва тарқатиш хусусияти уларнинг $n \geq m$ бўлганда кириш $\left(x_1^i, x_2^i, ..., x_n^i\right),\ i = 0,...,2^{n-1},$ ва чиқиш $\left(y_1^j, y_2^j, ..., y_m^j\right),\ j = 0,...,2^{m-1},$ битлар бирикмалари блокларининг чинлик жадвалидаги текс тақсимланганлигини аниқлаш билан аниқланади;

– акслантиришларнинг кириш блокларига мос чиқиш блокларини ўзаро боғлиқсиз – псевдотасодифий бўлиши уларни чизиқсизлигини таъминлайди;

– кириш блокларига мос чиқиш блокларини чинлик жадвалида текс тақсимланганлиги, яъни а) шартни бажарилиши

акслантиришнинг мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш самарадорлик, корреляцияга мосланувчанлик [3- 5,6] каби хоссаларини таъминлайди.

4. Критерий 4) алгоритм акслантиришларига тескари акслантиришлардан фойдаланиб амалга оширилиши мумкин бўлган криптоҳужумларга бардошликни таъминлайди, ҳсусан ПТКК блокининг бир қисмини ёки қисимларини билган ҳолда генератор – алгоритм калитини аниқлашни чеклайди.

Асосий акслантиришларининг биртомонламалик хусусиятига эга бўлмаслиги уларга нисбатан тескари акслантиришлардан фойдаланиб амалга оширилиши мумкин бўлган криптоҳужумларни яратишга шароит туғдиради.

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 акслантиршни амалий жиҳатдан мураккаб бўлишини таъминлайди. Шунинг учун алгоритм акслантиришларининг кўп алфавитли бўлишини текшириш лозим [3,4].

5. Критерий 5) шифрлаш (гаммалаштириш) калитининг етарли узун бўлишини таъминлайди, натижада калит алфавити элементларидан тузилган тўпламнинг қуввати етарли катта бўлиб, кўп алфавитли шифрлаш жараёнининг самарали амалга оширилиши таъминланади.

Алгоритм етарли узун даврга эга бўлган кетма-кетлик ишлаб чиқишни таъминланмаслиги кўп алфавитли шифрлаш жараёнининг самарали амалга оширилиши натижасини бермайди.

Псевдотасодифий кетма-кетлик $c_1c_2c_3c_4...c_8c_9...$ даври узинлиги унинг бирор $i=N$ номергача бўлган элементларини кейинги $i=N+1$ дан бошлаб $2N$ гача айнан такрорланмаслигини текшириш билан амалга оширилади. Бунинг учун псевдотасодифий кетма-кетликни $c_1c_2c_3c_4...c_8c_9...$ бирор $i=N=2^m, m=1,2,...;$ *масалан* $m>10$, бўлган қисми ажратилиб, кетма-кетликдаги қатнашиши мумкин бўлган белгилар ва белгилар бирикмаларини частотаси ҳисобланади. Агар бу частоталар қийматлари тенг ёки тенглари сони етарли кўп бўлса, псевдотасодифий кетма-кетлик даври λ-узунлигини аниқлаш оралиғи $2^{m-1}\le\lambda\le2^{m+1}$ бўлиши мумкин. Акси ҳолда λ-узунлик учун: $\lambda<2^{m-1}$ ёки $\lambda>2^{m+1}$ бўлиши мумкин. Бу таклиф этилган қоидадан фойдаланиш амалий жиҳатдан қулай бўлиб, “псевдотасодифий кетма-кетлик даври λ-узунлигини аниқлашнинг эҳтимоллик усули” деб юритилиши мумкин.

6. Критерий 6) ишлаб чиқилган ПТКК блокининг гаммалаштириш шифрлаш жараёни калити сифатида криптобардошли бўлишини таъминлайди.

Ишлаб чиқилган ПТКК блокининг бир битдан, икки битдан, уч битдан, ярим байт ва ҳокозо қисм блокларидан иборат кетма-кетлиги текис статистик тақсимот кўрсаткичига эга бўлмаса, ишлаб чиқилган ПТКК блокининг гаммалаштириш шифрлаш жараёни калити сифатида криптобардошли бўлишини таъминламайди.

Ишлаб чиқилган ПТКК блокининг қисм блокларидан иборат кетма-кетлигининг текис статистик тақсимот кўрсаткичига эга бўлишининг ўзи унинг шифрлаш жараёни калити сифатида криптобардошли бўлишини таъминламайди. Текис статистик тақсимот кўрсаткичига эга бўлишдан ташқари тасодифийлик хусусиятига ҳам эга бўлиши лозим. Бу хусусият статистиканинг тасодифийлик тестлари ёрдамида текширилади [3,4]. Кейинги пунктда шу ҳақида тўлароқ тўҳталинади.

7. Критерий 7) ишлаб чиқилган ПТКК блокининг қисм блоклари кетма-кетлигини тасодифийлигини етарли даражада юқори бўлишининг омилидир.

Псевдотасодифий кетма-кетликнинг гамма элементлари (бит, ярим байт, байт, қисм блоклари) барча бошқа элементларининг ҳиссаси орқали ҳосил қилиниши (силжитиш регистрлари асосида ишлаб чиқариладиган тасодифий кетма-кетлик каби) бажарилмаса – аралашиш самарали бўлмаса, ишлаб чиқилган ПТКК блокининг қисм блоклари кетма-кетлигини тасодифийлигини етарли даражада юқори бўлиши таъминланмайди.

Псевдотасодифий кетма-кетмакетлик элементларининг ва элементлари бирикмаларининг тақсимотини тасодифийликка текширишнинг “Хи-квадрат” критерийсини тадбиқи қуйидагича амалга оширилади.

Бирор жараён натижаларининг барча мумкин бўлган ҳолатлари $y_1, y_2, ..., y_k$, сони k та бўлиб, бу жараён бир-бирига боғлиқсиз ҳолда n марта ўтказилсин, $n>k$. Шунда, $y_1, y_2, ..., y_k$ - ҳолатларни, уларнинг n марта ўтказилган жараёнда, бир хил сонда такрорланишидан (текис тақсимотдан ёки бир хил частотага эга бўлишдан) қанчалик четланганлигини баҳолаш масаласи қуйидагича ечилади. Бунинг учун қуйидагича белгилашлар киритилади:

p_s - жараён натижаси y_s бўлишининг эҳтимоллик қиймати;

Y_s - жараён натижаларининг y_s ҳолатга тегишли бўлганлари (тенглари) сони.

Бу белгилашларга кўра “Хи-квадарат” деб аталувчи тақсимот критерийси ушбу

$$V=\sum_{s=1}^{k}\frac{(Y_s-np_s)^2}{np_s},$$

формула орқали аниқланади.

Агар жараён n мартадан бир неча марта ўтказилганда, ҳар доим $y_1, y_2, ..., y_k$ - ҳолатлар тенг Y_i мартадан такрорланса (текис тақсимланган ёки бир

хил частотали бўлса), яъни $Y_1 = Y_2 = ... = Y_k$ бўлса, у ҳолда $p_1 = p_2 = ... = p_k = \frac{1}{k}$, деб хулоса қилинади ва

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \sum_{s=1}^{k} \frac{\left(\frac{n}{k} - \frac{n}{k}\right)^2}{\frac{n}{k}} = 0$$

тенглик ўринли бўлади. Амалдаги аксарият жараёнларда бундай ҳолат кузатилмайди, яъни бирор жараён бир-бирига боғлиқсиз равишда n марта ўтказилганда: $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ ҳолат кузатилмайди. Шунинг учун $y_1, y_2, ..., y_k$ - ҳолатларни рўй бериш эҳтимолликлари бир хил $p_1 = p_2 = ... = p_k = \frac{1}{k}$ бўлиб, тажриба бир-бирига боғлиқ бўлмаган равишда n марта ўтказилганда, бу ҳолатларнинг рўй бериши сони мос равишда $Y_1, Y_2, ..., Y_k$ бўлса, у ҳолда ушбу

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2$$

формула $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ бўлган тенг тақсимотдан $Y_1, Y_2, ..., Y_k$ -тенг бўлмаган тақсимотни ўртача квадратик четланишини ифодалайди. Бу охирги формуладаги $\left(Y_s - \frac{n}{k}\right)$ - ифода бирор ўзгармас сон билан чегараланган, яъни $\left|Y_s - \frac{n}{k}\right| \le C = const \cdot$

Шунинг учун, жараённи амалга оширишнинг адекват модели тузилиб ва параметрлари қийматларини ўзгартириб, унинг кечиш жараёнини ифодаловчи ҳисоб-китобларни дастурий автоматлаштириб, етарли даражада кўп марта такрорланилса, яъни $n \to \infty$ бўлса, ушбу муносабатлар ўринли

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2 \le \frac{k}{n} \sum_{s=1}^{k} C^2 = \frac{(kC)^2}{n} \to 0.$$

Бу охирги муносабатдан, бирор генератор орқали ҳосил қилинган псевдотасодифий кетма-кетликнинг даври етарли узун бўлиб, барча мумкин бўлган битлар, байтлар ва қисм блокларининг тақсимоти деярли текис (тенг тақсимланган) бўлса, у ҳолда “Хи-квадарат” тақсимот критерийсининг бу кетма-кетликка нисбатан қиймати нолга яқин бўлиб, унинг тасодифийлик даражаси юқори бўлади деб ҳулоса қилинади.

Псевдотасодифий битлар кетма-кетлиги ишлаб чиқилган бўлиб, унинг даври узунлиги λ икки сонига каррали бўлсин, яъни $\lambda = 2^t$, t –бирор фиксирланган натурал сон.

Битлар кетма-кетлигининг тасодифийлигини текшириш учун қуйидагилар аниқлаб олинади:

1) ПТКК элементларининг қабул қилиши мумкин бўлган қийматлари “0” ва “1” иборат, яъни (s): 0 1 ;

2) Бу қийматларни қабул қилиш эҳтимоллиги (p_s): $\frac{1}{2}$ $\frac{1}{2}$;

3) Кузатилаётган сон (Y_s): N_0 ва N_1 , бу ерда N_0 ва N_1 мос равишда $c_1c_2c_3c_4...c_8c_9...$ –псевдотасодифий кетма- кетликнинг дастлабки $\lambda = 2^t$ та битидан иборат блокида иштирок этувчи ноллар ҳамда бирлар сони бўлиб, улар йиғиндиси $N_0 + N_1 = \lambda$;

4) Кутилаётган сон (λp_s): $\frac{\lambda}{2}$ $\frac{\lambda}{2}$.

Жадвал кўринишида қуйидагича ифодалаб олиш мумкин:

s	0	1
p_s	$\frac{1}{2}$	$\frac{1}{2}$
Y_s	N_0	N_1
λp_s	$\frac{\lambda}{2}$	$\frac{\lambda}{2}$

Хи- квадрат тақсимоти формуласи бўйича:

$$V = \sum_{s=0}^{k-1} \frac{\left(Y_s - np_s\right)^2}{np_s}$$ ҳисобланади

Ушбу қаралаётган ҳолатда $k = 2;\ s \in \{0;1\}$;

$$p_0 = p_1 = \frac{1}{2};\ Y_0 = N_0;\ Y_1 = N_1;\ n = \lambda = 2^t;$$

у ҳолда, қуйидагича катталикка эга бўлинади:

$$V = \frac{\left(N_0 - 128\right)^2 + \left(N_1 - 128\right)^2}{128}.$$

Бу катталикни ҳисоблаш учун Хи-квадрат тақсимотининг критик нуқталари жадвалидан фойдаланилади.

“Хи-квадрат” критерийси жадвали $\nu = k - 1 = 2 - 1 = 1$ – сатридан V қиймат жойлашган оралиқ топилади. Агар V қиймат жадвал устунининг $p = 25\%$ дан $p = 75\%$, оралиғида бўлса, у ҳолда ПТКК ишлаб чиқарувчи генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифий деб қабул қилинади.

	p=1%	*p=5%*	*p=25%*	*p=50%*	*p=75%*	*p=95%*	*p=99%*
N=1	0.00016	0.00393	0.1015	0.4549	1.323	3.841	6.635
N=2	0.02010	0.1026	0.5754	1.386	2.773	5.991	9.210
N =3	0.1148	0.3518	1.213	2.366	4.108	7.815	11.34
N =4	0.2971	0.7107	1.923	3.357	5.385	9.488	13.28
N =5	0.5543	1.1455	2.675	4.351	6.626	11.07	15.09
N =6	0.8721	1.635	3.455	5.348	7.841	12.59	16.81
N =7	1.239	2.167	4.255	6.346	9.037	14.07	18.48
N =8	1.646	2.733	5.071	7.344	10.22	15.21	20.09
N =9	2.088	3.325	5.899	8.343	11.39	16.92	21.67
N =10	2.558	3.940	6.737	9.342	12.55	18.31	23.21
N =11	3.053	4.575	7.584	10.34	13.70	19.68	24.72
N =12	3.571	5.226	8.438	11.34	14.85	21.03	26.22
N =15	5.229	7.261	11.04	14.34	18.25	25.00	30.58
N =20	8.260	10.585	15.45	19.34	23.83	31.41	37.57
N =30	14.95	18.49	24.48	29.34	34.80	43.77	50.89
N =50	29.71	34.76	42.94	49.33	56.33	67.50	76.15
N >50	$\upsilon+\sqrt{2\upsilon}x_p+\frac{2}{3}x_p^2-\frac{2}{3}+O\left(\frac{1}{\sqrt{\upsilon}}\right)$						
x_P =8	-2.33	-1.36	-0.674	0.00	0.674	1.64	2.33

Гарчанд псевдотасодифий генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифийликка “Хи-квадрат” критерийси бўйича текширилганда ижобий жавоб олинган бўлса ҳам, ундан кўра ишончли ва мукаммал бўлган жавоб олиш учун қаралаётган битлар кетма-кетлигини бошқа мавжуд тасодифийлик тестларига ҳам текшириб кўриш лозим. Бу критерийларга текширув натижаларида қанчалик кўп ижобий жавоблар олинса, критерий шунчалик яхши натижа деб қаралади.

Бундан ташқари қуйидаги жараён ҳам тасодифийликка текширишда чиқариладиган хулосанинг ижобийлигига сезиларли даражада таъсир кўрсатади, яъни псевдотасодифий генератор ёрдамида ишлаб чиқилган калитларнинг амалиётда ўрнатилган бардошсиз калитлардан ўртача квадрат четланишининг ўртача қийматини ифодаловчи жараён.

Псевотасодифий генератор ёрдамида ҳосил қилинган калит блоки:

$k = k_1k_2...k_n = k_1k_2...k_{2^t}$, бу ерда $k_i \in \{0;1\}$,

i=1,2, …, $n = \lambda = 2^t$,

Юқорида келтирилган критерий бўйича тасодифийликка текширилган ва қониқарли жавоб олинган бўлсин. Амалиёт жараёнида шифртизимлар билан ишлашда аниқланган бардошсиз калитларни $k_{н1}, k_{н2}, ..., k_{нт}$, каби белгилаймиз. Псевотасодифий генератор ёрдамида ҳосил қилинган калит блоки: $k = k_1k_2...k_n = k_1k_2...k_{2^t}$ ва амалиёт жараёнида бардошсиз деб топилган $k_{н1}, k_{н2}, ..., k_{нт}$, калитларнинг фарқи кўриб ўтилади:

$r_1 = k_{н1} \oplus k = r_1(1)r_2(1)...r_{2^t}(1)$, бу фарқ бўйича мос равишда 0 ва 1 битлар сони $N_0(1)$, $N_1(1)$;

$r_2 = k_{н2} \oplus k = r_1(2)r_2(2)...r_{2^t}(2)$, бу айирма бўйича мос равишда 0 ва 1 битлар сони $N_0(2)$, $N_1(2)$; ва ҳоказо

$r_m = k_{нm} \oplus k = r_1(m)r_2(m)...r_{2^t}(m)$, бу айирма бўйича мос равишда 0 ва 1 битлар сони $N_0(m)$, $N_1(m)$; бу катталиклардан фойдаланган ҳолда, қуйидагиларни ҳисоблаймиз:

$$V_1 = \frac{(N_0(1)-128)^2 + (N_1(1)-128)^2}{128};$$

$$V_2 = \frac{(N_0(2)-128)^2 + (N_1(2)-128)^2}{128};$$

$$V_m = \frac{(N_0(m)-128)^2 + (N_1(m)-128)^2}{128};$$

$$V = \frac{V_1 + V_2 + ... + V_m}{m}.$$

“Хи-квадрат” критерийси жадвали $\nu = k-1 = 2-1 = 1$, сатридан V - қиймат жойлашиш оралиғини топамиз. Агар V қиймат жадвал устунининг $p = 25\%$ дан $p = 75\%$, оралиғида бўлса, у ҳолда псевдотасодифий генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифий деб олинади.

Иккитадан битлар кетма-кетлигининг тасодифийлигини текшириш учун қуйидагилар аниқлаб олинади:

1) ПТКК элементларининг қабул қилиши мумкин бўлган қийматлари “00”, “01”, “10” ва “11” иборат, яъни (s): 00 01 10 11 ;

2) Бу қийматларни қабул қилиш эҳтимоллиги

(p_s): $\frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}\ \frac{1}{4}$;

3) Кузатилаётган сон (Y_s): $N_{00}\ N_{01}\ N_{10}$ ва N_{11}, бу ерда $N_{00}+N_{01}+N_{10}+N_{11}=\lambda=2^t$;

4) Кутилаётган сон (λp_s): $\frac{\lambda}{4}\ \frac{\lambda}{4}\ \frac{\lambda}{4}\ \frac{\lambda}{4}$.

Жадвал кўринишида қуйидагича ифодалаб олиш мумкин:

s	00	01	10	11
p_s	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
Y_s	N_{00}	N_{01}	N_{10}	N_{11}
λp_s	$\frac{\lambda}{4}$	$\frac{\lambda}{4}$	$\frac{\lambda}{4}$	$\frac{\lambda}{4}$

Ушбу параметрларга:

$k=4;\ s\in\{00;01;10;11\};$

$p_0=p_1=p_2=p_3=\frac{1}{4};\ Y_0=N_{00};\ Y_1=N_{01};$

$Y_2=N_{10};\ Y_3=N_{11};\ n=\lambda=2^t;$ эга бўлган ҳолда “Хи-квадрат” критерийси қўлланилиши юқоридаги каби амалга оширилади. Худи шулар каби учтадан битлар, ярим байт ва ҳоказо байтлар учун ҳам “Хи-квадрат” критерийсини тегишли ҳолда қўлланилиши мумкин.

Шундай қилиб калитни ифодаловчи ПТКК блок элементлари ва элементлари бирикмаларининг кетма-кетмакетлиги тақсимотини тасодифийликка текширишга “Хи-квадрат” критерийси қўлланилиши усули модели ишлаб чиқилди.

Олинган натижалар таҳлили. Узликсиз шифрлаш алгоритми туркуми учун криптобардошликни **з**арурийлик мезонлари шартларини текширишга асос бўлувчи математик модел, тавсия этилган таъмоиллар ва воситалар акслантиришларни тегишли мезонлар бўйича таҳлил этиш имкониятини беради.

“Псевдотасодифий кетма-кетлик даври λ-узунлигини аниқлашнинг эҳтимоллик усули” деб юритилиши мумкин бўлган қоида таклиф этилди.

ПТКК блок элементлари ва элементлари бирикмаларининг кетма-кетмакетлиги тақсимотини тасодифийликка текширишга “Хи-квадрат” критерийси қўлланилиши усули тўла ишлаб чиқилди. Улар дастурий таъминотлари яратилиши бардошлиликнинг зарурийлик мезонларини текширишнинг самарали амалга оширилишини таъминлайди.

Хулоса. Олинган натижалардан узликсиз туркумдаги шифрлаш алгоритмларининг бардошлиги зарурийлик мезонлари шартларини амалда текширишда илмий асосланган қўлланма сифатида фойдаланилиши мумкин.

Шартларини текширишга асос бўлувчи математик ёндошув усуллари, модел, тавсия ва воситалар акслантиришларни тегишли мезонлар бўйича таҳлил этишнинг таъмоилларини белгилайди.

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

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., 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.

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

Акбаров Давлатали Егиталиевич доктор физико-математических наук. Кокандский государственный педагогический институт.

E-mail: bardosh9295@mail.ru

Бекмуродов Улугбек Бахром угли старший – преподаватель. Самаркандский филиал Ташкентского университета информационных технологий

E-mail bardosh9295@mail.ru,

Мадаминов Эркин Комилович – инженер. Кокандский государственный педагогический институт.

E-mail: bardosh9295@mail.ru

Умаров Шухратжон Азизжонович – старший преподаватель. Ферганский филиал Ташкентского университета информационных технологий.

E-mail: sht003@umail.uz

D. E. Akbarov, U. B. Bekmurodov, E. K. Madaminov, Sh.A.Umarov

Checking the necessary conditions for the criterion of cryptographic stability of continuous encryption algorithms

In article deals with the solution of prolems to develop scientifically validated models of means for checking necessary conditions the criterion for the cryptographic stability of continuous encryption algorithms and their applications. The basic principles of solving problems are revealed and outlined.

Keywords: continuous encryption, crypto stability criterion, basic transformations, nonlinearity, regularity, balance, severe avalanche effect, correlation immunity, pseudo randomness, one-sidedness.