**Scientific reports of Bukhara State University**

Volume 2
Issue 1 *BSU 2019 issue 1*

Article 3

3-27-2019

# METHODS OF CHECKING THE NECESSARY CONDITIONS OF CRYPTIC RESISTANCE OF HESH FUNCTION ALGORITHM

Davlatali Yegitaliyevich Akbarov
*Dosent at the department of mathematics at Kokand State Pedagogical Institute, candidate of physical-mathematical science*

Shukhratjon Azizjonovich Umarov
*Senior teacher at the department of information technologies at the branch of Fergana Institute of Tashkent Informational Technological University*

**УДК 681.3**

# ХЭШ-ФУНКЦИЯ АЛГОРИТМИНИНГ КРИПТОБАРДОШЛИК ЗАРУРИЙЛИК МЕЗОНЛАРИНИ ТЕКШИРИШ УСУЛЛАРИ

# МЕТОДЫ ПРОВЕРКИ НЕОБХОДИМЫХ УСЛОВИЙ КРИПТОСТОЙКОСТИ АЛГОРИТМА ХЕШ-ФУНКЦИИ

# METHODS OF CHECKING THE NECESSARY CONDITIONS OF CRYPTIC RESISTANCE OF HESH FUNCTION ALGORITHM

**Akbarov Davlatali Yegitaliyevich**
*Dosent at the department of mathematics at Kokand State Pedagogical Institute, candidate of physical-mathematical science*
**Umarov Shukhratjon Azizjonovich**
*Senior teacher at the department of information technologies at the branch of Fergana Institute of Tashkent Informational Technological University*

**Таянч сўзлар:** хэш-функция, криптобардошликнинг зарурийлик мезонлари, бир томонлик хусусияти, мантиқий амаллар, мантиқий функциялар, жадвалли алмаштиришлар, матрицали акслантиришлар, чизиқсизлик, регулярлик, мувозанатлашганлик, корреляцияга мосланувчанлик ва қатъий кескин ўзгариш.

**Ключевые слова:** хеш-функция, необходимые условия криптостойкости, свойства односторонности, логические операции, логические функции, табличные замены, матричные преобразования, нелинейность, регулярность, сбалансированность, корреля-ционная иммунность, строгий лавинный эффект.

**Key words:** hash function, necessary conditions for cryptographic stability, one-way properties, logical operations, logical functions, table replacements, matrix transformations, nonlinearity, regularity, balance, correlation immunity, strict avalanche effect.

**Аннотация**

*Мақолада бит ёки байт бирликларида ифодаланган ихтиёрий чекли узунликдаги маълумотни бирор олдиндан қайд этилган – фиксирланган нисбатан кичик узунликдаги блокка сиқиб акслантирувчи хэш-функция алгоритмининг криптобардошлик критерий-ларини текширишнинг воситаларини яратиш масалалари ечимлари асослари ёритил-ган.*

**Аннотация**

*В статье представлены методы решения задач, определяющие условия крипто-графической стойкости алгоритма хеш-функции, преобразующей произвольную огра-ниченную длину электронного сообщения, выраженного в битах или байтовых едини-цах.*

**Abstract**

*The article deals with the foundations of the methods of solving problems of checking the criterion of cryptographic strength of a hash function algorithm that transforms an arbitrary bounded length of an electronic message expressed in bits or byte units.*

**Кириш.** Хэш-функциянинг криптографик восита сифатида келиб чиқиш зарурияти, таърифи, унга қўйиладиган талаблар, татбиқлари билан боғлиқ масалалар ҳамда улар ечими ҳақида манбаларда тўла маълумот берилган [1,2,3]. Хэш-функция деб бит ёки байт бирликларида ихтиёрий чекли узунликдаги маълумотни бирор олдиндан қайд этилган – фиксирланган нисбатан кичик узунликдаги блокка сиқиш акслантиришига айтилади.

Хэш-функциялар:

1) катта ҳажмдаги маълумотлар устида статистик тажрибаларни ўтказишда ва натижалари ўзгармаганлигини текшириш имкониятини таъминлаган ҳолда қисқа ҳажмдаги хэш-қиймат кўринишда сақлашда;

2) мантиқий ва ҳисоблаш қурилмаларини тўғри ишлаётганлигини катта ҳажмдаги кириш ҳамда мос чиқиш блоклари билан солиштириб, тест шаклида текширишда;

3) катта ҳажмдаги электрон ахборотни тез қидириб топиш алгоритмларини тузишда;

4) маълумотлар базасидаги электрон ахборотнинг бутунлигини, яъни ўзгармаган-лигини текшириш каби масалаларни ечишда қўлланилади.

**Асосий қисм. Масаланинг қўйилиши.** Ушбу мақолада хэш-функция алгоритмларига қўйиладиган криптобардошликнинг зарурийлик шартларини ёки критерийларини текширишнинг воситалари: математик модель, фундаментал қоида ва тавсия, тамоиллар ифодаси ишлаб чиқилиши масаласи қўйилади ҳамда унинг ечимлари тадқиқ қилинади.

**Масаланинг ечилиши.** Бир томонламалик хусусиятли (калитли бўлганда унинг узунлигига ҳам боғлиқ бўлган): бир томонлик хусусияти маълумотларни шифрлаш алгоритми (МША) негизида бўлган ҳамда мантиқий амаллар, сиқиш жадвали, мантиқий функциялар, $\oplus$ – XOR амали, параметрга боғлиқ ҳолда бажариладиган амаллар каби акслантиришларга асосланган хэш-функция алгоритмларининг криптабардошлигини таъминловчи талаблар ёки критерийлар қуйидагилардан иборат [4]:

1) хэш-функция алгоритми очиқ (маълум) бўлиб, унинг криптобардошлиги акслантиришларининг хусусиятларига боғлиқ, яъни калитли хэш-функция бўлганда калитнинг махфийлиги унинг узунлигига ҳам боғлиқ ва 256 битдан кам эмас;

2) ихтиёрий чекли узунликдаги $X$-матнга қўллаш мумкинлиги таъминланган бўлиши керак;

3) хэшлаш натижаси – хэш-функция қиймати тайинланган узунликдаги қийматда бўлиб, $(256+32\times l)$, $l=0,1,2,\ldots<\infty$, яъни 256 битдан кам эмас;

4) ихтиёрий берилган $x$ бўйича хэшлаш – хэш-функция қиймати $h(x)=H$ осон ҳисобланадиган бўлиши лозим;

5) ихтиёрий берилган хэш-функция қиймати $H$ бўйича $h(x)=H$ тенгликни қаноатлантирувчи $x$ матнни ҳисоблаб топиш имконияти мураккаб (бир томонламалик хоссаси) бўлиши зарур;

6) олинган $x$ ва $y\neq x$ матнлар учун $h(x)\neq h(y)$ бўлиши таъминланган(коллизияга бардошлилик хоссаси) бўлиши лозим;

7) акслантирилувчи блоклар узунликлари 256 битдан кам эмас: $k=k_1k_2...k_N$, $k_i\in\{0;1\}$, $N=32\times l$, $l=4,5,\ldots<\infty$ ҳамда алгоритм акслантиришлари микропроцессор, микроконтроллер ва компьютер ҳисоблаш технологиялари имкониятларидан самарали фойдаланишга мос бўлиши лозим;

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

9) асосий акслантиришлари оралиқ акслантириш натижалари номаълум бўлганда биртомонламалик хусусиятига эга бўлиши керак.

Хэш-функция алгоритмларининг криптабардошлигини таъминловчи талаблар – критерийлар таснифи:

1. 1-критерий алгоритм криптобардошлигига шубҳа бўлмаслигини таъминлаб, Кирхгофс тамойилига риоя қилинганлигини билдиради.

Хэш-функция алгоритмининг очиқ (маълум) бўлмаслиги, алгоритм криптобардош-лигига шубҳа туғилишига сабаб бўлади, шунингдек, калитли хэш-функция бўлганда унинг узунлиги 256 битдан кам бўлиши, барча мумкин бўлган калитларни танлаб чиқиш имкониятига замин бўлиши мумкин. Бу шартларни текшириш бевосита барча фойда-ланувчиларга алгоритмнинг криптографик хусусиятларини атрофлича ошкор ва тўла баён этиш билан амалга оширилади.

2. 2-критерий алгоритмнинг амалий татбиқи имкониятларини кенг қамровли бўлишини таъминлайди.

Ихтиёрий чекли узунликдаги *x*-матнга қўллаш мумкин бўлмаслиги алгоритмнинг амалий татбиқи имкониятларини чеклайди.

3. 3-критерий хэш-функция қиймати узунлигини $(256+32\times l)$ бит $l=0,1,2,\ldots<\infty$ бўлиши, яъни 256 битдан кам бўлмаслигини талаб этиш билан амалга ошириладиган криптоҳужумларга бардошликни таъминлашга имконият берувчи асос бўлади.

Хэшлаш натижаси – хэш-функция қиймати 256 битдан кам бўлиши мумкин бўлган ҳолатларни танлаб чиқиш билан амалга ошириладиган криптоҳужумларга бардошли бўлиш эҳтимолини камайтиради.

Ушбу келтирилган шартларни текшириш бевосита барча фойдаланувчилар учун алгоритмнинг криптографик хусусиятларини атрофлича ошкор ва тўла ёритилганлиги билан ифодаланади.

4. 4-критерий катта ҳажмдаги матнларга татбиқида алгоритмнинг тез ишлашини таъминлайди.

Ихтиёрий берилган *x* бўйича хэшлаш – хэш-функция қийматини $h(x)=H$ мураккаб ҳисоблашларга боғлиқлиги катта ҳажмдаги матнларга татбиқида алгоритмнинг самарасиз ишлашига олиб келади. Шартни текшириш алгоритмдаги акслантиришларни электрон ҳисоблаш қурилмалар кўринишидаги моделларини самаралиги билан аниқланади. Асосий акслантиришларининг мантиқий амаллар, жадвалли алмаштиришлар, мантиқий функциялар каби моделларга эгалиги ҳамда самарали аралаштириш ва тарқатиш хусусиятлари текширилади. Самарали аралаштириш ва тарқатиш хусусиятлари акслантиришларнинг мумкин бўлган барча кириш блокларига жуфт-жуфти билан ҳар хил чиқиш блокларини мос қўйилганлигини текшириш билан амалга оширилади.

5. 5-критерий алгоритм акслантиришларининг бир томонламалик хоссасига эга бўлиши лозимлигини билдиради: берилган хэш қийматга эга бўлган маълумот матнини топишнинг мураккаб бўлиши кераклигини – фабрикация имкониятининг мавжуд эмаслиги-ни таъминлайди.

Ихтиёрий берилган хэш-функция қиймати *H* бўйича $h(x)=H$ тенгликни қаноатланти-рувчи *x* матнни ҳисоблаб топиш имкониятини мураккаб (бир томонламалик хоссаси) бўлмаслиги фабрикация имконияти – коллизия учун замин бўлади.

Бу критерий шартлари асосий акслантиришлар математик моделларининг тескари акслантириш моделларига эга эмаслигини кўрсатиш билан амалга оширилади [5], [6]. Хусусан:

*а*) блоклар мос битлари устида мантиқий амаллар билан аниқланган акслантириш-лардаги мантиқий амал чинлик жадвалидаги “0” ва “1” ларни тенг (текис) тақсимланганли-ги, масалан

| $x/y$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $x/y$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 1 |

| $x/y$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 0 |

| $x/y$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 0 |

*б*) битлар бирикмаларини жадвалли алмаштиришларда ҳам шифр-белгиларнинг тенг (текис) тақсимланганлиги, масалан икки битли бирикмалар учун

| $x/y$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 00 | 11 | 10 | 01 | 00 |
| 01 | 10 | 01 | 00 | 11 |
| 10 | 01 | 00 | 11 | 10 |
| 11 | 00 | 11 | 10 | 01 |

*в*) мантиқий функциялар чинлик жадвалида мумкин бўлган барча кириш блокларига мос чиқиш блоки қийматларининг – шифр-белгиларнинг тенг (текис) тақсимланганлиги, яъни ушбу $Y = f(X) : GF(2)^n \to GF(2)^m$ акслантиришда $n > m$ бўлиб, унинг чинлик жадвали ифодаси қуйидагича

| $x_1 x_2 x_3$ | $x_1 x_2$ |
|---|---|
| 0=0 0 0 | 0 1 =1 |
| 1=0 0 1 | 0 0 =0 |
| 2=0 1 0 | 1 1 =3 |
| 3=0 1 1 | 1 0 =2 |
| 4=1 0 0 | 1 1 =3 |
| 5=1 0 1 | 0 0 =0 |
| 6=1 1 0 | 0 1 =1 |
| 7=1 1 1 | 1 0 =2 |

*г*) матрицали $A_{n\times n}$ акслантиришларда унинг иккита сатр ёки устун элементларининг пропорционал ёки тўртбурчакли матрица $A_{n\times m}$, $n \neq m$, эканлигини, яъни хусусиятларни текшириш билан эришилади, бу ерда $i \neq j$, $p \neq 0$.

$$A_{n\times n} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1i} = pa_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2i} = pa_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nj} = pa_{nj} & \dots & a_{nn} \end{pmatrix} \quad \text{ёки} \quad A_{n\times m} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

6. 6-критерий бир хил хэш-қийматга эга бўлган маълумотлар жуфтини топишнинг мураккаб эканлиги – коллизияга бардошликни билдиради, шунингдек, маълумот ва унинг хэш-қиймати берилганда, хэш-қиймати шунга тенг бўладиган бошқа маълумотни танлаш мураккаб бўлишини – модификациянинг имконияти йўқлигини билдиради.

Олинган *x* ва *y*≠*x* матнлар учун *h*(*x*)≠*h*(*y*) бўлиши таъминланмагани коллизияга бардошлилик хоссасининг таъминланмаганлигини билдириб, коллизия топиш имконияти борлигини билдиради. Яъни бир хил хэш-қийматга эга бўлган маълумотлар жуфтини топишнинг мураккаб эмаслиги – коллизияга бардошсизлигини билдиради. Шунингдек, маълумот ва унинг хэш-қиймати берилганда, хэш-қиймати шунга тенг бўладиган бошқа маълумотни танлаш имкониятининг бўлиши – модификациянинг имконияти борлигини билдиради.

Критерийни таъминланганлигини хеш-функция алгоритми бўйича жуфт-жуфти билан ҳар хил бўлган барча блокларга $x_i = \left(x_1^i x_2^i \dots x_{256}^i\right)$, $x_j^i \in \{0;1\}$, $j = 1,\dots,256$; $i = 0,1,\dots,2^{256}-1$; жуфт-жуфти билан ҳар хил бўлган хеш-қиймат блокларини $y_i = \left(y_1^i y_2^i \dots y_{256}^i\right)$ $y_j^i \in \{0;1\}$, $j = 1,\dots,256$; $i = 0,1,\dots,2^{256}-1$, мос қўйилганлигини текшириш билан амалга оширилади. Барча мумкин бўлган блоклар бўйича текшириб чиқиш имконияти йўқлиги учун имкон даражасида тасодифий танлов асосида кўриб чиқиш тавсия этилади.

7. 7-критерий барча мумкин бўлган блокларни танлаб чиқиш билан амалга ошириладиган криптоҳужумларни чеклайди, зарурият туғилганда калитни узайтириб, алгоритм базавий акслантиришлари асосларини сақлаб қолган ҳолда уни самарали модификациялаш имкониятини беради. Унинг аппарат қурилмаларини яратилишига қулайлик туғдиради ва тез ишлашини таъминлашга асос бўлади. Шу критерийни таъминланганлигини аниқлашга бевосита алгоритм акслантиришлари таркибий тузилишини таҳлил қилиш билан эришилади.

8. 8-критерий алгоритм акслантиришларининг криптоҳужумларга бардошли бўлишини таъминлаш учун зарур.

Асосий акслантиришларининг самарали аралаштириш ва тарқатиш хусусиятига эга бўлмаслиги, яъни акслантиришларининг: чизиқсизлик, мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш самарадорлик, корреляцияга мосланувчанлик каби хоссаларга эга бўлмаслиги алгоритм акслантиришларига кенг қамровли криптоҳужум воситаларини ишлаб чиқиш имкониятини беради.

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 блокларининг мос қўйилиши – регулярликни таъминлайди. Шунингдек, жуфт-жуфти билан ҳар хил бўлган барча мумкин бўлган кириш блокларига мумкин бўлган чиқиш блокларининг мос қўйишини тенг (текис) тақсимланганлиги – мувозанатлашганлигини аниқлаш орқали амалга оширилади. Ҳақиқатан ҳам, бу тасдиқнинг тўғрилигини, қулайлик учун кириш ва чиқиш блоклари узунлиги тўртга тенг бўлганда биектив акслантириш бўлган ҳолат учун кўриб ўтилади. Мувозанатлашганлик хусусияти таъминланган ҳолат учун ҳам биективликдаги каби хоссаларни ўринли эканлигини бевосита ҳисоблашлар натижаларини тегишли таърифларга мослигини ўрнатиш билан исботланади.

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:

**1-жадвал**

| $x_1\ x_2\ x_3\ x_4$ | $f_1\ f_2\ f_3\ f_4$ |
|---|---|
| 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 |
| 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 |

**2-жавдал**

| $f_1\ f_2\ f_3\ f_4$ | $x_1\ x_2\ x_3\ x_4$ |
|---|---|
| 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 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 буль функция ифодалари қуйидагича [3]:

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

$$f_1 = (\overline{x}_1 \overline{x}_2 \overline{x}_3 x_4) \oplus (\overline{x}_1 x_2 \overline{x}_3 \overline{x}_4) \oplus (\overline{x}_1 x_2 \overline{x}_3 x_4) \oplus (\overline{x}_1 x_2 x_3 \overline{x}_4) \oplus$$

$$\oplus (x_1 \overline{x}_2 \overline{x}_3 x_4) \oplus (x_1 \overline{x}_2 x_3 \overline{x}_4) \oplus (x_1 x_2 \overline{x}_3 \overline{x}_4) \oplus (x_1 x_2 x_3 x_4);$$

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

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

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

Бу акслантиришлар асосида кетма-кет мумкин бўлган ушбу кириш блокларида

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

тегишли ҳисоблашларга кўра 1-жадвал ва 2-жадвал ҳосил қилинади.

Буль функцияларни ҳамда уларга мос 1-жадвал ва 2-жавдал таҳлил қилиниб, 3-критерий ва 4-критерий шартларини текшириш мумкин.

Чинлик жадвали 1-жадвал бўйича барча $f_i$, $i = 1,2,3,4$; устунлардаги “0” ва “1” лар 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, яъни кириш блоклари битларининг ўзгариши чиқиш блокларининг ўзгариши билан статистик боғлиқ эмаслиги кўринади. Бундан акслантиришнинг корреляцияга мосланувчанлик ва қатъий кескин ўзгариш самарадорлик хоссаларини таъминланганлиги тегишли таърифларга мос равишда келиб чиқади [5]. Бунинг учун корреляцияга мосланувчанлик ва қатъий кескин ўзгариш самарадорлик $Y = f(X): GF(2)^n \to GF(2)^m$ ёки $Y = f(X): GF(2)^n \to GF(2)^n$ акслантиришларда ихтиёрий кириш блокининг $x = (x_1 x_2 ... x_n)$ бирор $k$ $(1 \le k < n)$ та ўзгарувчиларини фиксирлаганда фиксирланмаган ўзгарувчилари учун регулярлик ёки мувозанатлашганлик хоссаларини текшириш билан аниқланади. Шунда, кириш блокининг $x = (x_1 x_2 ... x_n)$ бирор $x_j$ $(1 \le j \le n)$ ўзгарувчиси қиймати ўзгарса, мос чиқиш блоки қиймати ҳам кескин ўзгариши кузатилади.

1-жадвал бўйича аниқланган $Y = f(X): GF(2)^4 \to GF(2)^4 -$ акслантиришни аниқловчи буль функциялар $f_i$, $i = 1,2,3$ ифодаларида $\overline{x}_i = x_i \oplus 1$ алмаштириш қилиниб, фақат $x_i$ ўзгарувчиларни конъюнкциясидан иборат ҳадларга боғлиқ

ифодаларга эга бўлинади. Ҳадларида $x_i$ ўзгарувчиларнинг қатнашганлиги сони билан улар чизиқсизлиги даражаси аниқланади. Кўрилаётган акслантириш мисолида ҳар бир $f_i$ , $i=1,2,3$ ифодаларида ушбу ҳад $x_1x_2x_3x_4$ қатнашган, $f_4$ ифодасида $x_1x_2x_3\overline{x_4}$. Бундан ташқари, бевосита ҳисоблаш ва соддалаштиришлардан сўнг бу ифодаларнинг чизиқсиз буль функциялар эканлигига ишонч ҳосил қилиш мумкин.

Келтирилган мисолдаги $Y=f(X):GF(2)^4\to GF(2)^4$ сюректив эканлигидан келтириб чиқарилган юқоридаги статистик боғлиқсизлик ҳамда текис тақсимот билан боғлиқ ҳолда қилинган хулосалар чизиқли ва дифференциал криптоҳужум турларини самарасиз бўлишини таъминлайди.

9. 9-критерий алгоритм акслантиришларига тескари акслантиришлардан фойдала-ниб, амалга оширилиши мумкин бўлган криптоҳужумларга бардошлиликни таъминлайди.

Асосий акслантиришлари оралиқ акслантириш натижалари номаълум бўлганда биртомонламалик хусусиятига эга бўлмаслиги алгоритм акслантиришларига тескари акслантиришлардан фойдаланиб, амалга оширилиши мумкин бўлган криптоҳужумларга замин бўлади.

Хэш-функция алгоритми учун ҳам, бардошликни таъминловчи зарурийлик амалий етарлилик шарти критерийлари тўла бажарилганда ҳам криптоҳужум воситасини яратишга таянч бўлувчи манбаларни аниқлаш мумкин. Бу манбалар улар қўлланиладиган амал-ларнинг содда ҳисоблашлардан иборат эканлигида бўлиб, микропроцессор, микро-контроллер ва компьютер ҳисоблаш технологиялари имкониятларидан самарали фойдаланишга мос бўлган акслантиришлар математик моделларини аниқ ифодаси борлиги билан боғлиқ.

Бардошли алгоритмлар учун дешифрлаш калитларининг танлаш криптоҳужум усулини қўллаш имконияти ҳар доим бор, аммо унинг самарали бўлишига эришиш криптоаналитикнинг биртомонламалик хусусиятига эга бўлган акслантиришларни тескарисини танлаб топиш маҳоратига, ҳисоблаш техника ва технологияларининг нечоғли самарали бўлишига боғлиқ.

Бу критерийнинг бажарилганлигини бевосита алгоритм акслантиришлари таркибий тузилишини таҳлил қилиш билан аниқланади.

Хеш-функция алгоритмлари ихтиёрий чекли узунликдаги матнни ташкил этувчи белгилари сони 256 тадан кам бўлмаган фиксирланган блокка биртомонламалик, самарали аралаштириш ва тарқатиш хусусиятига эга асосий (базавий) акслантиришларни матн блокларига такроран қўллаш (итерациялаш) билан амалга ошириладиган жараён-дир. Мутахассислар томонидан тан олинган стандарт хеш-функция алгоритмлари калитсиздир. Шундай бўлиши моҳиятан тўғри, чунки калитсиз бўлиши ва алгоритмнинг очиқ бўлиши фойдаланувчилар орасида ўзаро ишончсизликка олиб келувчи ҳолатларни келтириб чиқармайди. Бундан ташқари, хешланадиган матннинг энг охирги хешланувчи блоклари сифатида унга қуйидагилар бириктирилади:

а) *тўлдириш битларини қўшиш*– агар охирги блок узунлиги 256 битдан кичик бўлса, 256 битгача ноль ёки бўшлиқ белгиси билан тўлдирилади;

б) *маълумот узунлигини қўшиш*– тўлдириш битлари билан биргаликда битлар сони билан аниқланадиган маълумот узунлигини билдирувчи блок, яъни тўлдирилган маълумотнинг битлари сони чекли mod $2^{256}$ майдонда ҳисобланиб, ҳосил бўлган қиймат 256 битлик блок кўринишида бирлаштирилади;

в) *назорат йиғиндисини қўшиш* – 2-босқич натижасига берилган маълумотнинг назорат йиғиндисини билдирувчи 256 битлик блок бирлаштирилади. Назорат йиғиндисини билдирувчи блок, охирги тўлиқ бўлмаган блок ноль ёки бўшлиқ белгиси билан тўлдирил-гандан кейин ҳосил бўлган кенгайтирилган матннинг барча блоклар

қийматларининг ўнлик саноқ системасидаги йиғиндисини mod $2^{256}$ бўйича ҳисобланади ва у охирги хешланадиган блок сифатида бириктирилади.

Бу бириктириладиган қўшимча блоклар хеш-функциянинг коллизияга бардошлигини оширади. Хэш-функцияларга қуйидаги криптоҳужум турлари мавжуд [1,7]:

1. Хэш-функция алгоритмида қатнашган акслантиришлар бўйича криптоҳужум;
2. Алгоритм акслантиришларининг дифференциал криптотаҳлил усулига бардошли-лигига ҳужум;
3. Матнларнинг тўқнашуви усули асосидаги криптоҳужум;
4. Барча мумкин бўлган очиқ матн вариантларни танлаш асосидаги ҳужум.

Бу криптоҳужумларни амалга ошириш симметрик блоклаб шифрлаш алгоритмлари-даги каби хусусиятларни ҳисобга олган ҳолда амалга оширилади.

**Хулоса**. Хэш-функция алгоритмининг криптобардошлигини таъминловчи зарурийлик мезонлари шартларини текширишга асос бўлувчи тегишли математик ёндошув усуллари, модель, тавсия ва воситалар унинг акслантиришларини таҳлил этишнинг тамойилларини белгилайди [7]. Хэш-функция акслантиришларини тегишли мезонлар бўйича таҳлил этиш-нинг тамойиллари фан-техника ва технологияларнинг ютуқларига, янги асосли алго-ритмлар яратилиши каби жараёнларга боғлиқ ҳолда тизимли равишда бойитиб борилади.

Олинган натижалар хэш-функция алгоритмлари бардошлиги зарурийлик мезонлари шартларини амалда текширишда илмий қўлланма учун асосдир.

## REFERENCES

**1. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V.** Osnovi kriptografii: Uchebnoe posobie. - M.: Gelios ARV, 2002. - 2-e izd. - 480 s.

**2. Shnayer B.** Prikladnaya kriptografiya. Protokoli, algoritmi, isxodnie teksti na yazike Si. - M.: TRIUMF, 2003. - 816 s.

**3. Akbarov D.E.** Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi. - Toshkent: O'zbekiston markasi, 2009. - 432 b.

**4. Akbarov D.E., Muxtarov F.M., Siddiqov A.A.** Kriptotahlil masalalariga tizimli yondoshuv asoslari va ularni yechish usullari. - Farg'ona: 2014. - 143 b.

**5. Akbarov D.E., Umarov Sh.A.** Algoritm xesh-funktsii s novimi bazovimi preobrazova-niyami //Вісник Національного технічного університету України "Київський політехнічний інститут". Серія: Приладобудування. - 2016. - № 51 (1). – С. 100-108. DOI: https://doi.org/10.20535/1970.51(1). 2016.78112

**6. Akbarov D.E., Umarov Sh.A., Xasanov X.M.** Axborot muhofazasini ta'minlash vositalarining ba'zi masalalari yechimlariga mantiqiy amallar tatbiqi //Farg'ona politexnika institui. Ilmiy-texnika jurnali. 2016. - № 20, maxsus nashr. - B. 29-33.

**7. Akbarov D.E, Umarov Sh.A.** Working out the new algorithm enciphered the data with a symmetric key //Siberian Federal University. Engineering & Technologies. 2016. 9(2). – P. 214-224. DOI: https://doi.org/10.17516/1999-494X-2016-9-2-214-224.