

ISSN 2010-9857

O'zbekiston Respublikasi Axborot texnologiyalari va  
kommunikatsiyalarini rivojlantirish vazirligi  
Toskent axborot texnologiyalari universiteti



Министерство по развитию информационных  
технологий и коммуникаций Республики Узбекистан  
Ташкентский университет информационных  
технологий

Ministry for development of information  
technologies and communications of the  
Republic of Uzbekistan  
Tashkent University of Information Technologies



**TATU XABARLARI**  
**ВЕСТНИК ТУИТ • TUIT BULLETIN**

4(36)/2015

Toshkent - Tashkent - Tashkent

# TATU XABARLARI ВЕСТНИК ТУИТ TUIT BULLETIN

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETINING  
ILMIY-TEXNIKA VA AXBOROT-TAHLILY JURNALI

JURNAL 2007 YILDA TASHKIL  
ETILGAN.  
BIR YILDA TO'RT MARTA  
NASHR QILINADI

4(36)/2015

<http://jurnal.tuit.uz>

## Tahrir haya'ti:

Muxitdinov X.A. – bosh muharrir  
Bobomurodov H.M. – bosh muharrir o'rinbosari  
Xakimov Z.T. – bosh muharrir o'rinbosari  
Maxmudov M.M.  
Fayzullayev A.N.  
Kamalov Yu.K.  
Musayev M.M.  
Radjabov T.D.  
Abduraxmanov Q.P.  
Usmonov R.N.  
G'aniyev S.K.  
Raxmatullayev M.A.  
Nishonboyev T.N.  
Zokirova F.M.  
Qodirov A.M.  
Xaldjigitov A.A.  
Nishonov A.X.  
Tashev K.A.  
Raxmatov F.A.  
Davronbekov D.A.  
Raxmanov Q.S. – mas'ul kotib

«TATU xabarlari» jurnali («Вестник ТУИТ», «TUIT Bulletin») O'zbekiston matbuot va axborot agentligida 2007 yil 22-yanvarda 0204 - son bilan ro'yxatdan o'tgan.

O'zR OAK tomonidan doktorlik dissertatsiyalari yuzasidan ilmiy maqolalar chop etilishi lozim bo'lgan ilmiy jurnallar ro'yxatiga kiritilgan (2008 yil 2 yanvardagi 001-I-sonli buyruq).

Tahririyat manzili:  
100202, Toshkent sh., Amir Temur ko'chasi, 108, B505-xona.  
Tel.: (+99871) 238-64-53  
E-mail: [tuit\\_xabar@tuit.uz](mailto:tuit_xabar@tuit.uz)  
Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

TOSHKENT - 2015

<b>INFORMATIKA VA AXBOROT TEXNOLOGIYALARI</b>		
Odami qomati antropometrik belgilarini masofadan o'lish tizimi	<i>Abdulkarimova M.A.</i>	3
Tibbiyot axborot tizimlari uchun ma'lumotlar bazasini loyihalash	<i>Abdulmononov A.A.</i>	7
TIAV-multimedia tizimlari axborot resurslariga ishlov berish jarayonlarini modellashtirish usullari	<i>Abduraxmonov K.P., Beknazarova S.S.</i>	12
Videotaxvirda odam qo'l harakati koordinatlarini aniqlash va kompyuterni masofadan boshqarish	<i>Mamarajov O.A., Raxmanov H.E.</i>	19
Neyron tarmoqlarini inson nutqini idrok etish masalalarida qo'llanilishi	<i>Musayev M.M., Baxronov Sh.N.</i>	24
AKT sohasida kadrlar tayyorlashda dasturlash tillarini o'rgatuvchi tizimlarning o'rni	<i>Raxmanov Q.S., Abidova Sh.B., Xojiyev S.N.</i>	30
oliy ta'lim muassasalari dekanat faoliyatini avtomatlashtirish tizimi	<i>Mahmanov O.Q.</i>	34
WDM tizimlarida optik aloqa kanallarining sifatini baholash usullarini tanlash	<i>Mirzaimova G.X.</i>	38
Elektron axborot resurslarining bilimlar bazasi uchun bilimlarni ajratib olish usullari	<i>Raximov N.O.</i>	42
<b>INFOKOMMUNIKATSION TARMOQLAR VA TIZIMLAR</b>		
Keyingi avlod tarmoqlarda abonent kirish pog'onaning ishonchlik parametrlarining tadqiqoti	<i>Nishanbayev T.N., Muradova A.A.</i>	47
Transport jarayoni dispatcher xizmatida axborot oqimlarining modeli	<i>Turgunov M.R.</i>	54
<b>RADIOTEKNIKA, RADIOALOQA VA TELERADIOESHITTIRISH</b>		
Axborotlarni uzatish raqamli tizimlari uchun modulyatsiya turini tanlash	<i>Jisupov Ya.T.</i>	58
<b>MATEMATIK MODELASHITIRISH VA DASTURLASH</b>		
Tizim ta'sirchanligini tahlil etish usullari	<i>Mirzayev A.N.</i>	64
Extimollik avtomatlaridagi o'tish ehtimolliklari haqidagi taxminlarni tekshirish kriteriyasi	<i>Islamova O.A., Chay Z.S.</i>	68
Kardiosignal generatori: dasturiy imitatsiyaning o'ziga xos xususiyatlari va tibbiyot masalalarida qo'llanish imkoniyatlari	<i>Kasimova Sh.T., Usarov A.B.</i>	72
Funksional rad etish shakllanishida dasturiy ta'minotning ishonchlik ko'rsatkichlarini tanlash	<i>Mirzayev D.A.</i>	76
Aylanalardan va to'rtburchaklardan iborat fraktallarni qurishning rekursiv algoritmlari	<i>Nuraliyev F.M., Anarova Sh.A., Mullamaxamedova M.A., Sultonov D.U.</i>	82
Algoritma rasceta korrelyatsionmax svyazey mejdu tematicheskimi slojami gas telekommunikatsionmax sistem	<i>Oteniyazov R.I., Allamuratova Z.J.</i>	88
Yurak - qon tomirlari tizimida biomexanik jarayonlarni matematik modellashtirish	<i>Sadaddinova S.S., Abduqayumov B.</i>	93
Qat'iy mas axborotlar muhitida vebga yo'naltirilgan tizimlarida individuallashtirishning matematik usuli	<i>Xamidov V.S.</i>	97
<b>AXBOROT XAVFSIZLIGI</b>		
Yangi o'rniga qo'yish shiflash algoritmi va uning apparat qurilmasini samarali usuli	<i>Akbarov D.Ye., Umarov Sh.A., Mustarov F.M., Atadjanov Sh.Sh.</i>	105
Biometrik templeyd xavfsizligida ta'minlashda xatoliklarni to'g'rilovchi kodlarning muhimligi va ularning tahlili	<i>Xudoykulov Z.T., Islamov Sh.Z., Xalmuratov O.U.</i>	111
Tub sonlarni generatsiyalashning extimollik algoritmlari tadqiqi va tahlili	<i>Mahmudov A.A., Turayev X.S.</i>	117
"Elektron hukumat" tizimida axborot xavfsizligini ta'minlashning muammolari	<i>Abduraxmanov A.A., Nazirov A.A., Xudoykulov Z.T.</i>	122
Gubka sxemasiga asoslangan ma'lumot autentifikatsiya kodi algoritmi	<i>Kuryazov D.M.</i>	127
<b>MIKROELEKTRONIKA VA SXEMOTEXNIKA</b>		
Kremniyda elektr nafaol kislorod va uglerod defekt va presipitatlarni yaralish mexanizmi	<i>Abduraxmonov K.P.</i>	132
Nosimmetrik elektrik kuchlanishlarda elektr tarmoqlari aloqa va telekommunikatsiya qurilmalarining ishlash tartibi	<i>Siddikov I.X., Borisova Ye. A., Amurova N. Yu.</i>	140
<b>Ilmiy ma'lumot</b>		
Yozish mahoratini o'qitish va baholashda qanday qilib muvaffaqiyatga erishish mumkin?	<i>Avezova D.D.</i>	144
Biplanetar mexanizmi quyosh energiya majmuasida qo'llanilishi	<i>Nurmatov A.S.</i>	148
Universitetlarda dasturlashni o'qitishning usullari	<i>Maxmudov A.Z., Abdulkarimov S.S.</i>	153

**ЗАЩИТА ИНФОРМАЦИИ  
INFORMATION SAFETY**

УДК 681.3

**ЯНГИ ЎРНИГА ҚЎЙИШ ШИФРЛАШ АЛГОРИТМИ ВА УНИНГ  
АППАРАТ ҚУРИЛМАСИНИ САМАРАЛИ УСУЛИ**

*Акбаров Д.Е., Умаров Ш.А., Мухтаров Ф.М., Атаджанов Ш.Ш.*

Мақолада аппарат қурилмаси яратилиши қулай ва самарали ҳамда криптобардошлилиги етарли даражада юқори бўлган янги ўрнига қўйиш шифрлаш алгоритми таклиф этилган. Унинг аппарат қурилмасини яратишнинг қулай ва самарали усули ишлаб чиқилган.

**Таянч иборалар:** криптография, микропроцессор, микроконтроллер, шифрпроцессор, шифрлаш, дешифрлаш, алгоритм, бул функция, криптобардош, симметрик, функционал схема.

В статье предлагается новый криптостойкий алгоритм шифрования замены, аппаратная реализация которого удобно и эффективно. Разработан эффективный метод создания его аппаратное средство.

**Ключевые слова:** криптография, микропроцессор, микроконтроллер, шифрпроцессор, шифрования, дешифрования, алгоритм, Булава функция, крипто стойкость, симметрический, функциональная схема.

In article the new crypto firmness algorithm of enciphering of the replacement, which hardware realization conveniently and effectively is offered. The effective method of creation its hardware is developed.

**Keywords:** cryptography, microprocessor, microcontroller, codeprocessor, enciphering, decoding, algorithm, Bul function, crypto firmness, symmetric, function chart.

**Кириш**

Аксарият криптографик аппарат (техник) воситалари микропроцессорлар, микроконтроллерлар ва махсулаштирилган процессорлар, яъни шифрпроцессорлар асосида яратилган. Бундай криптографик аппарат воситалари тўлиқ аппарат қурилма бўлмай, улар криптографик аппарат дастурий восита ҳисобланади. Чунки бундай криптографик аппарат дастурий воситасининг ишлаш жараёни микроконтроллер таркибидаги ёки алоҳида жойлашган доимий хотира қурилмасига ёзилган маълум бир криптографик алгоритмга боғлиқ бўлади. Демак, микропроцессор, микроконтроллер ва шифрпроцессорлар иштирокида йиғилган қурилмаларни криптографик аппарат дастурий воситалар туркумига киритиш мумкин. Шифрпроцессорларнинг ишлаш жараёнларида ўзига хос афзалликлар ва камчиликлар бор. Камчилиги шундаки, агар шифрпроцессорни ташкил этувчи бирор элемент ишдан чиқса, уни тўлиқ алмаштириш талаб этилади. Уларни тайёрлаш технологиялари мурраккаб шарт-шароитларни талаб қилади ва таннархи ҳам юқори бўлади. Аммо бундай камчиликлар, бугунги ахборот технологиялари ривожланган – жамиятнинг ижтимоий, иқтисодий, сиёсий ва бошқа барча соҳаларида ахборотнинг роли ортиб бораётган пайтда, ахборотни муҳофазасини таъминлашдан келиб чиқадиган манфаатдорлик эвазига қопланади. Шифрпроцессорларнинг афзаллик томонлари шундаки, уларнинг ички хотира қурилмасига олдиндан танланган бирон-бир шифрлаш алгоритмининг дастурини киритиш мумкин ва у шу киритилган шифрлаш алгоритми асосида ишлайди.

Ҳозирги кундаги янги технологиялар ёрдамида битта кристалда бир неча-юз миллион

электрон элементлардан ташкил топган шифрпроцессор тайёрлаш мумкин ва у ёрдамида бир вақтнинг ўзида бир неча амалларни бажариш имкониятлари мавжуд. Бундан ташқари, бу технология қурилмаларида амаллар бажарувчи элементлар сони камаюди ва ишлаш тезлиги ортади.

$2^5=32$ ,  $2^6=64$  ва ундан ортиқ  $2^n$ ,  $n=7,8,\dots$ ; разрядли универсал микропроцессорларнинг яратилиши ва ахборотни тўплаш, қайта ишлаш, ахборот-коммуникация тармоқларида кафолатли муҳофазасини таъминлаган ҳолда алмашиш технологиялари соҳаларида кенг тадбиқ этилиши, криптографик акслантиришларни амалга оширувчи махсуслантирилган электрон ҳисоблаш машиналаридан воз кечиб, битта ихчамлашган электрон платада йиғилган криптографик аппарат воситалариларга ўтишга сабабчи бўлди ва бўлмоқда. Бундай криптографик аппарат воситалари ўзининг қулай ва самарадорлиги билан махсуслантирилган ЭХМлардан афзал бўлмоқда. Бундай криптографик аппарат воситаларининг негизини, яъни ядросини шифрпроцессор ташкил этади. Унинг архитектураси микроЭХМнинг архитектурасидан иборат бўлиб, ўзининг (“ППЗУ – перепрограммируемое запоминающее устройство” –қайтадастурлаш хотира қурилмасига – ҚДХК) дастур қайта ёзиладиган хотира (ДҚЁХ, айрим манбаларда Flesh деб ҳам айтилади) қурилмасига ва доимий хотирасига олдиндан ёзиб қўйилган махсус буйруқлар тўпламига эгадир. Бу буйруқлар тўплами алгоритмнинг бажарилишини бошқаришда ва ички калитлар тизимини бошқаришда ишлатилади. Шифрпроцессор ўзининг ички, яъни қуйи сатҳидаги калитлар тизимига эга бўлиши аппарат қурилмадан маълумотнинг электромагнит тўлқин орқали тарқалишини олдини олади ва юқори сатҳидаги калитларни ҳосил қилишда қўшимча имконият яратади.

Дастурлаш ва қайта дастурлаш қурилмасига эга криптографик аппарат дастурий воситаларда шифрлаш алгоритми акслантиришларини уларда кўрсатилган амалларни бажаришдаги ҳисоб-китоблар орқали амалга оширилади. Акслантиришларни дастурий амалга оширишда уларда кўрсатилган амалларни бажаришга сарфланадиган вақт электр сигналларини жуда оз бўлсада тутилишига (узилишига) сабаб бўлади. Бундай тутилишлар шифрлаш акслантирилиши (сигналларни қайта ишлаш) жараёнлари тезлигининг камайишига сабаб бўлиб, аппарат дастурий қурилмаларнинг самарадорлигини пасайтиради.

Дастурлаш ва қайта дастурлаш қурилмаларидан фаркли ўлароқ шифрлаш акслантирилиши (сигналларни қайта ишлаш) жараёнлари фақат мантикий ва бошқа электрон элементлар орқали амалга ошириладиган аппарат қурилма воситаларида электр сигналларини тутилиши (узилиши) рўй бермай, акслантириш самарадорлиги тўла таъминланади [1].

Қуйида аппарат қурилмасини яратиш қулай ва самарали ҳамда криптобардошлилиги етарли даражада юқори бўлган янги ўрнига қўйиш шифрлаш алгоритми таклиф этилиб, унинг аппарат қурилмаси функционал тузилиши (схемаси) асослари ишлаб чиқилади.

**Асосий қисм**

Қуйидаги 1- жадвал асосида калит сифатида қаралиб амалга ошириладиган янги ўрнига қўйиш шифрлаш алгоритми ишлаб чиқилади, бу ерда  $0 \leq S_t \leq 2^n - 1$ ,  $n=8,9, \dots, N<\infty$ ;  $t=0,1,\dots,2n - 1$ .

1-жадвал.

Ўрнига қўйиш шифрлаш алгоритми

0	1	2	...	t	...	j	...	$2^n - 1$
$S_0$	$S_1$	$S_2$	...	$S_t$	...	$S_j$	...	$S_{2^n - 1}$

Энди эса таклиф этилган ўрнига қўйиш акслантириши аппарат қурилмасини функционал схемаси ёритилади. Аппарат қурилманинг ихчам, қулай ва самарали

яратилишини таъминлаш учун калитни ифодаловчи жадвалли алмаштиришнинг буль функциялари тузиб олинади (2-жадвал).

2-жадвал

Буль функцияларининг чинлик жадвали

$x_1 x_2 \dots x_{n-1} x_n$	$f_1$	$f_2$	...	$f_{n-1}$	$f_n$
0 = 0 0 ... 0 0	$S_0 = s_1(0)$	$s_2(0)$	...	$s_{n-1}(0)$	$s_n(0)$
1 = 0 0 ... 0 1	$S_1 = s_1(1)$	$s_2(1)$	...	$s_{n-1}(1)$	$s_n(1)$
...	...	...	...	...	...
$2^n - 2 = 1 1 \dots 1 0$	$S_{2^n-2} = s_1(2^n - 2)$	$s_2(2^n - 2)$	...	$s_{n-1}(2^n - 2)$	$s_n(2^n - 2)$
$2^n - 1 = 1 1 \dots 1 1$	$S_{2^n-1} = s_1(2^n - 1)$	$s_2(2^n - 1)$	...	$s_{n-1}(2^n - 1)$	$s_n(2^n - 1)$

$n=8$  бўлганда 2-жадвал кўриниши куйидагича бўлади:

3-жадвал. Буль функцияларининг  $n=8$  бўлгандаги чинлик жадвали

$x_1 x_2 \dots x_7 x_8$	$f_1$	$f_2$	...	$f_7$	$f_8$
0 = 0 0 ... 0 0	$S_0 = s_1(0)$	$s_2(0)$	...	$s_7(0)$	$s_8(0)$
1 = 0 0 ... 0 1	$S_1 = s_1(1)$	$s_2(1)$	...	$s_7(1)$	$s_8(1)$
...	...	...	...	...	...
254 = 1 1 ... 1 0	$S_{254} = s_1(254)$	$s_2(254)$	...	$s_7(254)$	$s_8(254)$
255 = 1 1 ... 1 1	$S_{255} = s_1(255)$	$s_2(255)$	...	$s_7(255)$	$s_8(255)$

4-жадвал.

Буль функцияларининг  $n=256$  бўлгандаги чинлик жадвали

$x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$	$f_7$	$f_8$
0 = 0 0 0 0 0 0 0 0	81=	0	1	0	1	0	0	1
1 = 0 0 0 0 0 0 0 1	162=	1	0	1	0	0	1	0
...	...	...	...	...	...	...	...	...
254 = 1 1 1 1 1 1 1 0	101=	0	1	1	0	0	1	1
255 = 1 1 1 1 1 1 1 1	202=	1	1	0	0	1	0	1

Куйида мисол сифатида 4-жадвал кўрилади. Шифрлаш алгоритмлари акслантиришларини умумий ҳолда  $GF(2^n) = \{x = (x_1, x_2, \dots, x_n) \in X : x_i \in \{0;1\}\}$  –фазо элементларини бирор амал ёки амалларнинг чекли сондаги кетма-кетлиги орқали бошқа  $GF(2^n) = \{y = (y_1, y_2, \dots, y_n) \in Y : y_i \in \{0;1\}\}$  – фазо элементларига алмаштириш деб қараш мумкин ва у буль функциялар кўринишида куйидагича ифодаланади:

$$Y = f(X) : GF(2^n) \rightarrow GF(2^n).$$

Бу акслантириш ифодасидаги вектор-функция ушбу  $f(x) = \{f_1(x), f_2(x), \dots, f_n(x)\}$  кўринишида тасвирланади, бу ерда  $x_i, y_i \in GF(2)$ , яъни  $x_i, y_i \in \{0;1\}$ .

Акслантиришларнинг криптографик хусусиятлари очиқ маълумот блоки элементлари, “калит” деб аталувчи махфий параметр ва оралиқ алмаштиришлар натижалар блоки элементлари ҳамда улар устида бажарилиши керак бўлган амаллар буль функциялари хоссалари орқали ўрганилади [2].

Буль функция ифодалари учун алгебраик нормал форма деб аталувчи куйидаги

$$f(x) = a_0 \oplus \sum_{1 \leq i_1 \leq n} a_{i_1} x_{i_1} \oplus \sum_{1 \leq i_1 < i_2 \leq n} a_{i_1 i_2} x_{i_1} x_{i_2} \oplus \dots \oplus \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1 \dots i_k} \oplus \dots \oplus a_{12 \dots n} x_1 x_2 \dots x_n,$$

бу ерда  $x \in GF(2^n)$  ва коэффициент  $a \in GF(2)$ , кўринишдан фойдаланилади.

Шундай қилиб, бул функцияларнинг  $GF(2^n)$  - майдондаги алгебраик нормал форма ифодалари деганда  $x_1, x_2, \dots, x_n$  – ўзгарувчиларнинг барча мумкин бўлган кўпайтмаларини мос коэффициентлари  $a_{i_1 i_2 \dots i_k} \in \{0,1\}$  билан биргаликдаги ҳадларнинг  $\oplus$  – амали орқали йиғиндиси тушунилади.

Берилган  $f(x)$  функциянинг алгебраик нормал форма ифодасида қўшилувчиларнинг энг кўп ўзгарувчилар катнашган кўпайтмасидаги ўзгарувчилар сони бу функциянинг алгебраик чизиксизлик даражаси дейилади ва  $\deg(f)$  деб белгиланади.

Криптографик акслантиришларга мос келувчи бул функцияларнинг мувозанатлашганлик (баланслашганлик) ва регулярилик шартларини қаноатлантиришини таъминлаш масаласини ечиш уларнинг криптобардошлилиги билан боғлиқ бўлган муҳим талаблардан ҳисобланади. Бу шартларни бажарилиши блокли шифрлаш алгоритмлари акслантиришларига нисбатан статистик криптохужум турларини самарали амалга ошириш имкониятларини чеклайди. Алгоритм акслантиришлари криптографик хоссаларини таҳлил қилишда, уларга мос келувчи бул функцияларини қуриб, уларнинг баланслашганлик ва регулярилик хоссаларига эгаллигини таъминлаш блокли криптобардошли акслантиришларни яратиш имкониятини беради.

**1-таъриф [1].** Берилган  $f(x)$ – бул функция мувозанатлашган (баланслашган) дейилади, агар унинг чинлик жадвалида “0” ва “1” лар сони тенг бўлса, яъни ушбу муносабат

$$\#\{x \mid f(x) = 0\} = \#\{x \mid f(x) = 1\} = 2^{n-1}$$

ўринли бўлса.

**2-таъриф [1].** Агар  $X \in GF(2^m)$  – элементларнинг барча  $2^m$  та ҳар хил қийматларида  $Y$  – функция ўзининг  $GF(2^n)$ -майдондаги  $2^n$  та ҳар хил қийматларини роппа-роса  $\frac{2^n}{2^m} = 2^{n-m}$  мартадан қабул қилса,  $Y = f(X): GF(2^m) \rightarrow GF(2^n)$ ,  $n \geq m$ , акслантириш регуляри дейилади,

Бу таърифдан қуйдаги тасдиқ келиб чиқади.

**Тасдиқ [1].** Агарда  $Y = f(X): GF(2^m) \rightarrow GF(2^n)$ -акслантиришда  $n=m$  бўлиб, у регулярилик шартини қаноатлантирса, у биектив акслантириш бўлади, яъни бу функция ва унга тескари бўлган функция ўзаро бир қийматлилик хоссасига эга бўлади.

Таклиф этилган алгоритмда қалитни ифодаловчи жадвалли алмаштириш акслантиришининг чинлик жадвали ўзаро бир қийматлилик – биективлик хоссасига эга.

Қалитни ифодаловчи жадвалли алмаштиришнинг чинлик жадвалига мос келувчи бул функцияларнинг ифодаси ҳар бир  $f_i$  устун учун алоҳида тузилади.  $f_i$  га “1” (чин) қиймат берувчи ўзгарувчилар конъюнкциясидан иборат бўлган 128 та ҳаддан ташкил топган бўлиб, ўзгарувчи инкорига  $\bar{x}_i$  нол “0” қиймат, ўзгарувчининг ўзига бир “1” қиймат мос келади ва барча мумкин бўлган  $2^8 = 256$  та қийматларда чинлик жадвалининг  $f_i$ , ( $i=1,2,\dots,8$ ) га мос келувчи устунини ифодалади.

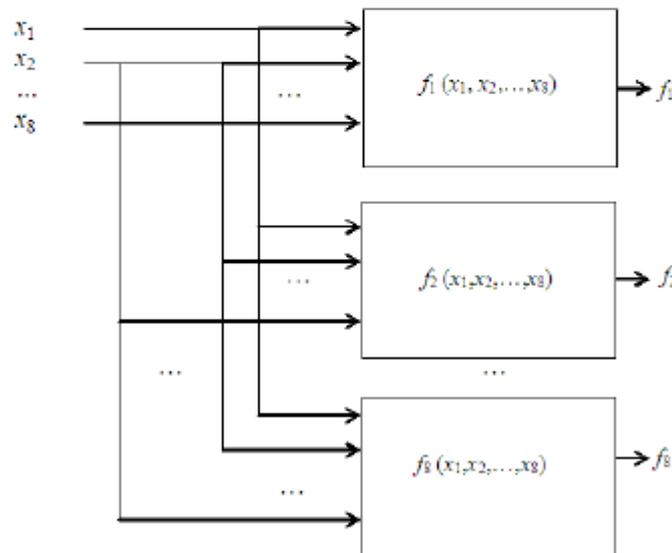
Юқорида  $n=8$  да мисол сифатида келтирилган чинлик жадвалига мос келувчи бул функциялари келтирилади:

$$\begin{aligned}
 f_1 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8); \\
 f_2 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8) \oplus \\
 &\quad \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8); \\
 f_3 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8); \\
 f_4 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus \dots; \\
 f_5 &= \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8); \\
 f_6 &= \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8); \\
 f_7 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8); \\
 f_8 &= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus \dots \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8).
 \end{aligned}$$

Буль функциялар ифодаларида  $\bar{x}_i = x_i \oplus 1$  алмаштириш бажарилиб ва соддалаштириб, унинг алгебраик нормал форма кўриниши олинади.

Бу ифодалардан фойдаланиб симметрик шифрлаш алгоритмлари ўрнига кўйиш алмаштиришларининг корреляцион иммунитетлик кўрсаткичи (даражаси), қатъий кескин ўзгариш самарадорлик тамойили – таркалиш тамойили даражалари каби баҳоланади [1,3].

Қуриб олинган буль функциялардан  $f_i$  ( $i=1,2,\dots,8$ ) фойдаланиб алгоритмнинг аппарат қурилмасини ихчам, қулай ва самарали функционал схемаси ишлаб чиқилади:

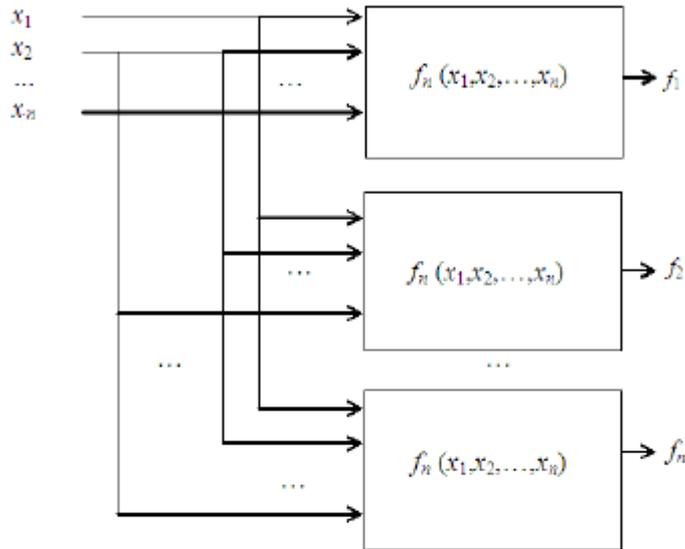


1-расм.  $f_i$  ( $i=1,2,\dots,8$ ) буль функциялардан фойдаланилган шифрлаш алгоритмнинг функционал схемаси

### Хулоса

Фойдаланилган адабиётлар рўйхатида келтирилган [1,2]–манбаанинг аппарат қурилмаларни яратиш усулларидадан фойдаланиб [3]–манбааларда келтирилган криптобардошли ҳамда акслантириш сигналларини оддий мантиқий электрон элементлар орқали тутилишсиз амалга ошириш имкониятини берувчи криптоалгоритмлар гоёларидан фойдаланиб, юқоридаги каби улар аппарат қурилмаларини ҳужжатли, овозли ва тасвири маълумотларнинг криптографик муҳофазасини таъминлаш учун ишлаб чиқиш мумкин.

Кириш  $(x_1, x_2, \dots, x_n)$  ва чиқиш  $(f_1, f_2, \dots, f_n)$ ,  $n=8, 9, \dots, N < \infty$  бўлганда 1-расмда келтирилган схема кўриниши қуйидагича бўлади:



2-расм. Умумий ҳолдаги  $f_i$  ( $i=1, 2, \dots, n$ ) бўлғи функциялардан фойдаланилган шифрлаш алгоритмнинг функционал схемаси

### АДАБИЁТЛАР

1. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – с. 448
2. Шалыто А.А. Логическое управление. Методы аппаратной и программной реализации. – Санкт-Петербург.: «БХВ-Петербург», 1999. – с. 779
3. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, “Ўзбекистон маркаси” 2009 – 434 б.
4. Акбаров Д.Е. Об одном алгоритме шифрования данных с симметричным ключом. //Инфокоммуникации: Сети-Технологии-Решения, 4(8)/2008, – с. 25-36.

<i>Abdulkarimova M.A.</i>	<i>eInfo-fans axborot texnologiyalari markazi davlat unitar korxonasi katta ilmiy xodimi</i>
<i>Abdumamonov A.A.</i>	<i>Toshkent tibbiyot akademiyasi Farg'ona filiali "Biofizika, sport va axborot texnologiyalari" kafedrası katta o'qituvchisi</i>
<i>Abduraxmonov Q.P.</i>	<i>TATU "Fizika" kafedrası professori</i>
<i>Abidova Sh.B.</i>	<i>TATU "Informatika asoslari" kafedrası assistenti</i>
<i>Anarova Sh.A.</i>	<i>TATU kuzuridagi dasturiy maxazotlar apparat-dasturiy majmaal yaratish markazi katta ilmiy xodim</i>
<i>Allamuratova Z.J.</i>	<i>TATU Nukuz filiali "Telekommunikasiya injiniringi" kafedrası assistenti</i>
<i>Abduqayumov B.</i>	<i>TATU talabasi</i>
<i>Akharov D.E.</i>	<i>TATU Farg'ona filiali "Axborot texnologiyalari" kafedrası dosenti</i>
<i>Atadjanov Sh.Sh.</i>	<i>TATU O'qov-uslubiy ishlar bo'yicha filiallar bilan ishlash bo'limi boshlig'i</i>
<i>Abduraxmanov A.A.</i>	<i>TATU katta ilmiy xodim tadqiqotchi</i>
<i>Amarova N.Ya.</i>	<i>TATU "Energiya ta'winoti" kafedrası katta o'qituvchisi</i>
<i>Avezova D.D.</i>	<i>TATU "Chet tillari" kafedrası assistenti</i>
<i>Abdulkarimov S.S.</i>	<i>TATU talabasi</i>
<i>Beknazarova S.S.</i>	<i>TATU "Audiovizual texnologiyalari" kafedrası katta o'qituvchi</i>
<i>Baxromov Sh.N.</i>	<i>TATU qashidagi radioelektron tizimlar va axborot texnologiyalari markazi katta mutaxassisi</i>
<i>Borisova E.A.</i>	<i>TATU "Energiya ta'winoti" kafedrası katta o'qituvchisi</i>
<i>Hojiyev S.N.</i>	<i>TATU magistranti</i>
<i>Hamidov V.S.</i>	<i>TATU "Fizika" kafedrası mudiri</i>
<i>Hadiykulov Z.T.</i>	<i>TATU "Axborot harfiyiligi" kafedrası assistenti</i>
<i>Halmuratov O.U.</i>	<i>TATU tadqiqotchi</i>
<i>Islomov Sh. Z.</i>	<i>TATU "Axborot harfiyiligi" kafedrası assistenti</i>
<i>Islamova O.A.</i>	<i>TATU "Oliy matematika" kafedrası katta o'qituvchisi</i>
<i>Kasimova Sh.T.</i>	<i>TATU "Informatika asoslari" kafedrası katta o'qituvchisi</i>
<i>Kariyazov D.M.</i>	<i>TATU qashidagi radioelektron tizimlar va axborot texnologiyalari Markazi katta o'qituvchisi</i>
<i>Mamaraaifov O.A.</i>	<i>TATU "Axborot texnologiyalarining dasturiy ta'winoti" katta ilmiy xodim</i>
<i>Musayev M.M.</i>	<i>TATU "Kompyuter tizimlari" kafedrası professori</i>
<i>Mohamamov O.Q.</i>	<i>O'zB Vazirlar Mahkaması kashidagi Oliy attestatsiya komissiyasi</i>
<i>Mirajimova G.H.</i>	<i>"OAK axborot-kommunikasiya texnologiyalarini joriy etish va rivojlantirish markazi" dasturchisi</i>
<i>Muradova A.A.</i>	<i>TATU "Telekommunikasiya injiniringi" kafedrası katta o'qituvchisi</i>
<i>Mirzayev A.N.</i>	<i>TATU "Telekommunikasiya injiniringi" kafedrası assistenti</i>
<i>Mullemmukamedova M.A.</i>	<i>TATU "Algoritmash va matematik modellash" kafedrası dosenti</i>
<i>Mirzayev D.A.</i>	<i>TATU katta ilmiy xodim izlanuvchi</i>
<i>Muktarov F.M.</i>	<i>TATU BKUK raisi</i>
<i>Mahmudov A.A.</i>	<i>TATU Farg'ona filiali "Axborot texnologiyalari" kafedrası mustaqil ilmiy tadqiqotchisi</i>
<i>Mahmudov A.Z.</i>	<i>TATU "Tizimli va amaliy dasturlash" kafedrası assistenti</i>
<i>Nishanbayev T.N.</i>	<i>TATU "Informatika asoslari" kafedrası assistenti</i>
<i>Nuraliyev F.M.</i>	<i>TATU "Ma'lumotlarni azalish tizimi va tarmoqlari" kafedrası professori</i>
<i>Nazirov A.A.</i>	<i>TATU "Televizion texnologiyalar" jukalveti dekani</i>
<i>Nurmatov A.S.</i>	<i>TATU "Axborot harfiyiligi" kafedrası assistenti</i>
<i>Oteniyazov R.I.</i>	<i>Abu Rayson Beraniy nomidagi DDTU "Neft va gaz obyektlarini loyihalash" kafedrası katta ilmiy xodimi</i>
<i>Raxmanov Q.S.</i>	<i>TATU "Kompyuter tizimlari" kafedrası assistenti</i>
<i>Raxmanov H.E.</i>	<i>TATU "Informatika asoslari" kafedrası mudiri</i>
<i>Raximov N.O.</i>	<i>TATU Samarqand filiali "Axborot texnologiyalari" kafedrası assistenti</i>
<i>Sultonov D.U.</i>	<i>TATU, Katta ilmiy xodim-izlanuvchi</i>
<i>Sadaddinova S.S.</i>	<i>TATU talabasi</i>
<i>Siddikov I.H.</i>	<i>TATU "Algoritmash va matematik modellash" kafedrası dosenti</i>
<i>Turgunov M.R.</i>	<i>TATU "Energiya ta'winoti" kafedrası katta o'qituvchisi</i>
<i>Turayev H.S.</i>	<i>TATU "Axborot texnologiyalari" kafedrası assistenti</i>
<i>Yusupov Ya.T.</i>	<i>TATU magistranti</i>
<i>Usarov A.B.</i>	<i>DDTU "Radiotexnik qurilmalar va tizimlar" kafedrası katta o'qituvchisi</i>
<i>Umarov Sh.A.</i>	<i>TATU talabasi</i>
<i>Chay Z.S.</i>	<i>TATU Farg'ona filiali "Axborot texnologiyalari" kafedrası katta o'qituvchisi</i>
	<i>TATU "Oliy matematika" kafedrası katta o'qituvchisi</i>

