ISSN 2010-9857

O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi
Toshkent 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 -Ташкент - Tashkent

ТАТУ ХАБАРЛАРИ
ВЕСТНИК ТУИТ
TUIT BULLETIN

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

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

4(36)/2015

http://jurnal.tuit.uz

«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
Qo‘lyozmalar taqrizlanmaydi va qaytarilmaydi.

TOSHKENT - 2015

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, алгортим, буль 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, алгортим, Булавая 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, codeprotsessor, enciphering, decoding, algorithm, Bul function, crypto firmness, symmetric, function chart.

Кириш

Аксарият криптографик аппарат (техник) воситалари микропроцессорлар, микроконтроллерлар ва махсуслаштирилган 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 мухофазасини 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 камаяди ва ишлаш тезлиги ортади.

2^5=32, 2^6=64 ва ундан ортиқ 2^n, n=7,8,…; 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 махсуслаштирилган электрон ҳисоблаш машиналаридан воз кечиб, битта ихчамлашган электрон платада йиғилган криптографик аппарат воситаларларга ўтишга сабабчи бўлди ва бўлмоқда. Бундай криптографик аппарат воситалари ўзининг қулай ва самарадорлиги билан махсуслаштирилган ЭҲМлардан афзал бўлмоқда. Бундай криптографик аппарат воситаларининг негизини, яъни ядросини шифрпроцессор ташкил этади. Унинг архитектураси микроЭҲМнинг архитектурасидан иборат бўлиб, ўзининг (“ППЗУ – перепрограммируемое запоминающее устройство” –қайтадастурлаш хотира қурилмасига – ҚДХҚ) 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 фарқли ўлароқ шифрлаш акслантирилиши (сигналларни қайта ишлаш) жараёнлари фақат мантиқий 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 $0 \le S_t \le 2^n - 1$, n=8,9, …, $N<\infty$; t=0,1,…,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	$S_0 = s_1(0)$	$s_2(0)$	...	$s_{n-1}(0)$	$s_{n-2}(0)$
1 = 0 0 … 0 1	$S_1 = s_1(1)$	$s_2(1)$	...	$s_{n-1}(1)$	$s_{n-2}(1)$
…			…		
2^n-2 = 1 1 … 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 … 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 қуйидагича 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 0 1
1 = 0 0 0 0 0 0 0 1	162= 1 0 1 0 0 0 1 0
…	…
254 = 1 1 1 1 1 1 1 0	101= 0 1 1 0 0 1 0 1
255 = 1 1 1 1 1 1 1 1	202= 1 1 0 0 1 0 1 0

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

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

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

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 қуйидаги

$$f(x) = a_0 \oplus \sum_{1 \le i \le n} a_i x_j \oplus \sum_{1 \le i_1 < i_2 \le n} a_{i_1 i_2} x_{i_1} x_{i_2} \oplus \ldots \oplus \sum_{1 \le i_1 < \ldots < i_k \le k} a_{i_1 \ldots i_k} \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n ,$$

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

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

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

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

1-таъриф [1]. Берилган $f(x)$– буль 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 $X \in GF(2^s)$ – элементларнинг барча 2^n та ҳар хил қийматларида Y – функция ўзининг $GF(2^n)$-майдондаги 2^m та ҳар хил қийматларини роппа-роса $\frac{2^n}{2^m} = 2^{n-m}$ мартадан қабул қилса, $Y = f(X): GF(2^s) \to GF(2^m)$, $n \ge m$, акслантириш регуляр дейилади,

Бу таърифдан қуйдаги тасдиқ келиб чиқади.

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

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

Калитни ифодаловчи жадвалли алмаштиришнинг чинлик жадвалига мос келувчи буль 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 $\overline{x_i}$ 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,…,8) га мос келувчи устунини ифодалайди.

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

$$f_1 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus .... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8);$$

$$f_2 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus .... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8) \oplus$$
$$\oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8);$$

$$f_3 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8);$$

$$f_4 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus ... \quad ;$$

$$f_5 = ... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8);$$

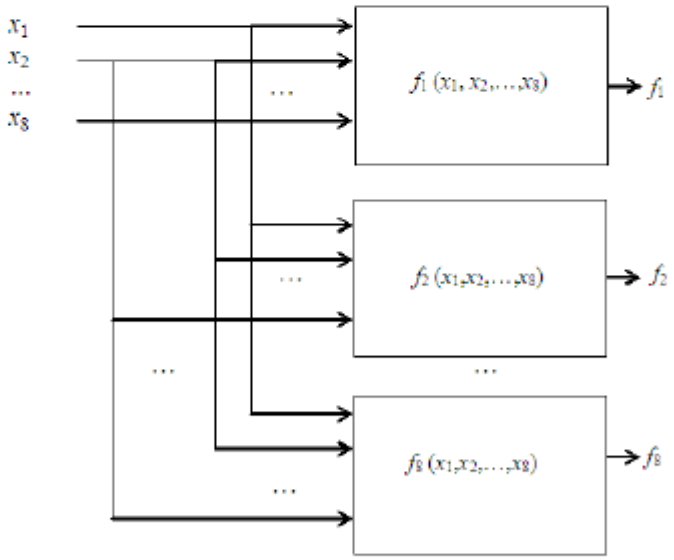
$$f_6 = ... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8);$$

$$f_7 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge x_8) \oplus .... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge x_8);$$
$$f_8 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6 \wedge \bar{x}_7 \wedge \bar{x}_8) \oplus .... \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6 \wedge x_7 \wedge \bar{x}_8).$$

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 қўйиш алмаштиришларининг корреляцион иммунистлик кўрсаткичи (даражаси), қатъий кескин ўзгариш самарадорлик тамойили – тарқалиш тамойили даражалари каби баҳоланади [1,3].

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

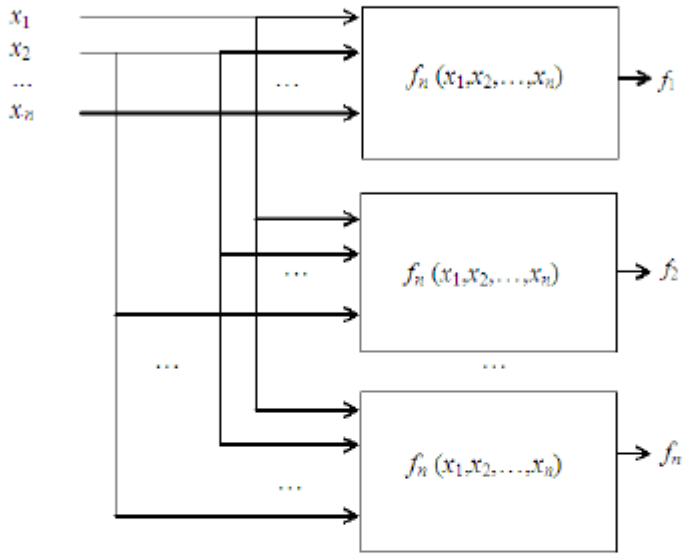


1-расм. f_i (i=1,2,…,8) буль функциялардан фойдаланилган шифрлаш алгоритмнинг функционал схемаси

Хулоса

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

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



2-расм. Умумий ҳолдаги f_i (i=1,2,…,n) буль 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.

Abdukarimova M.A.	*«Info-fanv axborot texnologiyalari markazi davlat unitar korxonasi katta ilmiy xodimi*
Abdumanonov A.A.	*Toshkent tibbiyot akademiyasi Farg'ona filiali "Biofizika, sport va axborot texnologiyalari" kafedrasi katta o'qituvchisi*
Abdurazmonov Q.P.	*TATU "Fizika" kafedrasi professori*
Abidova Sh.B.	*TATU "Informatika asoslari" kafedrasi assistenti*
Anarova Sh.A.	*TATU huzuridagi dasturiy maksulotlar apparat-dasturiy majmaalar yaratish markazi katta ilmiy xodim*
Allamuratova Z.J.	*TATU Nukus filiali "Telekommunikasiya injiniringi" kafedrasi assistenti*
Abduqayumov B.	*TATU talabasi*
Akbarov D.E.	*TATU Farg'ona filiali "Axborot texnologiyalari" kafedrasi dosenti*
Atadjanov Sh.Sh.	*TATU O'quv-uslubiy ishlar bo'yicha filiallar bilan ishlash bo'limi boshlig'i*
Abdurazmanov A.A.	*TATU katta ilmiy xodim tadqiqotchi*
Amanova N.Yu.	*TATU "Energiya ta'minoti" kafedrasi katta o'qituvchisi*
Avezova D.D.	*TATU "Chet tillari" kafedrasi assistenti*
Abdukarimov S.S.	*TATU talabasi*
Beknazarova S.S.	*TATU "Audiovizual texnologiyalari" kafedrasi katta o'qituvchi*
Baxronov Sh.N.	*TATU qoshidagi radioelektron tizimlar va axborot texnologiyalari markazi katta mutaxassisi*
Borisova E.A.	*TATU "Energiya ta'minoti" kafedrasi katta o'qituvchisi*
Hojiyev S.N.	*TATU magistranti*
Hamidov V.S.	*TATU "Fizika" kafedrasi mudiri*
Hudoykulov Z.T.	*TATU "Axborot havfsizligi" kafedrasi assistenti*
Halmuratov O.U.	*TATU tadqiqotchi*
Islomov Sh. Z.	*TATU "Axborot havfsizligi" kafedrasi assistenti*
Islamova O.A.	*TATU "Oliy matematika" kafedrasi katta o'qituvchisi*
Kasimova Sh.T.	*TATU "Iformatika asoslari" kafedrasi katta o'qituvchisi*
Kuryazov D.M.	*TATU qoshidagi radioelektron tizimlar va axborot texnologiyalari Markazi katta o'qituvchisi*
Mamaraufov O.A.	*TATU "Axborot texnologiyalarining dasturiy ta'minoti" katta ilmiy xodim*
Musayev M.M.	*TATU "Kompyuter tizimlari" kafedrasi professori*
Mahmanov O.Q.	*O'zR Vazirlar Mahkamasi huzuridagi Oliy attestasiya komissiyasi "OAK axborot-kommunikasiya texnologiyalarini joriy etish va rivojlantirish markazi" dasturchisi*
Mirazimova G.H.	*TATU "Telekommanikasiya injiniringi" kafedrasi katta o'qituvchisi*
Muradova A.A.	*TATU "Telekommanikasiya injiniringi" kafedrasi assistenti*
Mirzayev A.N.	*TATU "Algoritmlash va matematik modellashtirish" kafedrasi dosenti*
Mullamuhamedova M.A.	*TATU katta ilmiy xodim izlanuvchi*
Mirzayev D.A.	*TATU BKUK raisi*
Muktarov F.M.	*TATU Farg'ona filiali "Axborot texnologiyalari" kafedrasi mustaqil ilmiy tadqiqotchisi*
Mahmudov A.A.	*TATU "Tizimli va amaliy dasturlash" kafedrasi assistenti*
Mahmudov A.Z.	*TATU "Informatika asoslari" kafedrasi assistenti*
Nishanbayev T.N.	*TATU "Ma'lumotlarni uzatish tizimi va tarmoqlari" kafedrasi professori*
Nuraliyev F.M.	*TATU "Televizion texnologiyalar" fakulteti dekani*
Nazirov A.A.	*TATU "Axborot havfsizligi" kafedrasi assistenti*
Nurmatov A.S.	*Abu Rayxon Beruniy nomidagi TDTU "Neft va gaz obyektlarini loyixalashtirish" kafedrasi katta ilmiy xodimi*
Oteniyazov R.I.	*TATU "Kompyuter tizimlari" kafedrasi assistenti*
Raxmanov Q.S.	*TATU "Informatika asoslari" kafedrasi mudiri*
Raxmanov H.E.	*TATU Samargand filiali "Axborot texnologiyalari" kafedrasi assistenti*
Raximov N.O.	*TATU, Katta ilmiy xodim-izlanuvchi*
Sultonov D.U.	*TATU talabasi*
Sadaddinova S.S.	*TATU "Algoritmlash va matematik modellashtirish" kafedrasi dosenti*
Siddikov I.H.	*TATU "Energiya ta'minoti" kafedrasi katta o'qituvchisi*
Turgunov M.R.	*TATU "Axborot texnologiyalari" kafedrasi assistenti*
Turayev H.S.	*TATU magistranti*
Yusupov Ya.T.	*TDTU "Radiotexnik qurilmalar va tizimlar" kafedrasi katta o'qituvchisi*
Usarov A.B.	*TATU talabasi*
Umarov Sh.A.	*TATU Farg'ona filiali "Axborot texnologiyalari" kafedrasi katta o'qituvchisi*
Chay Z.S.	*TATU "Oliy matematika" kafedrasi katta o'qituvchisi*