ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Хизмат доирасида фойдаланиш учун
25 **-нусха**

Қўлёзма ҳуқуқида
004.056.55

Туйчиев Ғулом Нумонович

ТАКОМИЛЛАШГАН ФЕЙСТЕЛ ТАРМОҒИ ЯРАТИШ ВА УНИНГ ТАТБИҚЛАРИ

05.13.19 – Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги

техника фанлари номзоди илмий даражасини олиш учун тақдим этилган диссертация

А В Т О Р Е Ф Е Р А Т И

Тошкент–2011

Иш Ўзбекистон миллий университетида бажарилган.

Илмий раҳбар — физика-математика фанлари доктори, профессор **Арипов Мирсаид Мирсиддиқович**

Расмий оппонентлар: техника фанлари доктори, профессор **Хасанов Пўлат Фаттохович**

физика-математика фанлари номзоди **Курьязов Давлатёр Матякубович**

Етакчи ташкилот: Тошкент давлат техника университети

Ҳимоя Тошкент ахборот технологиялари университети ҳузуридаги Д.001.25.01 ихтисослашган ке[A]2011 йил «10» ноябр соат 11[00] да ўтадиган мажлисида

Манзил: 100084, То[T81 — A/2478 Туйчиев Г.Н. Тэкомиллэшган Фейстел тэрмаги... 6/4]кўчаси, 108, тел.: 238-64-15.

Диссертация бил[ ]университетининг кутубхо[ ]

Автор[ ]

Ихтисослашг[ ]

илмий котиби[ ]

ДИССЕРТАЦИЯНИНГ УМУМИЙ ТАВСИФИ

Мавзунинг долзарблиги. Ахборот технологияларининг жадал ривожланиб бориши билан ахборотни ҳимоялаш зарурияти келиб чиқди. Шу сабаб, республикамизда ҳам сўнгги йилларда криптография йўналишига бўлган қизиқиш тобора ортиб бормоқда ва йўналишни ривожлантиришга катта аҳамият берилмоқда. Бунга кейинги йилларда шифрлаш, хэш-функция, электрон рақамли имзо бўйича миллий стандартлар ишлаб чиқилганлиги, қабул қилинган бир нечта қонун ва меъёрий ҳужжатлар мисол бўлади.

Ҳозирда ахборот хавфсизлиги соҳасида Фейстел тармоғига асосланган криптоалгоритмлар кўплаб қўлланиб келинмоқда. Бу криптоалгоритмларга мисол қилиб Россия Федерацияси давлат стандарти ГОСТ 28147-89, Америка қўшма штатлари собиқ стандарти DES, шунингдек, 3DES, CAST, E2, Blowfish, FEAL, Lucifer, LOKI криптоалгоритмларни олиш мумкин. DES, 3DES, Blowfish криптоалгоритмлари ахборот алмашинувини муҳофаза қилиш протоколлари VPN, IPSec, SSL асосини ташкил этади. Фейстел тармоғининг афзаллиги шундан иборатки, маълумотни калит ёрдамида дешифрлашда шифрлаш алгоритмининг ўзидан фойдаланиб, шифрлаш раунд калитларини тескари тартибда қўллаш орқали амалга оширилади. Бу эса битта аппарат воситадан раунд калитлари жойлашиш тартибини ўзгартириш орқали шифрлаш ва дешифрлашда фойдаланиш имконини беради. Ҳисоблаш техникалари ривожланиши натижасида бугунги кунда қўлланиб келинаётган криптоалгоритмлар бардошлиги уларда қўлланилган акслантиришларга боғлиқ бўлмаган ҳолда калитларининг узунликларига нисбатан камаяди. Бу криптоалгоритмлар акслантиришларини сақлаб қолган ҳолда уларнинг калит ва блок узунлигини узайтириш, Фейстел тармоғи асосий афзалликларини сақлаб қолган ҳолда уни такомиллаштириш ва янги криптоалгоритмлар ишлаб чиқиш долзарблиги келиб чиқади.

Муаммонинг ўрганилганлик даражаси. Тадқиқот даврида Х.Фейстел томонидан яратилган тармоқ асосида янги тармоқ яратган ва унинг таҳлилига ҳисса қўшган олимлар J.M.Carroll, G.Chew, J.Choy, V.T.Hoang, S.Ibrahim, N.B.Idris, J.Kelsey, K.Khoo, M.A.Maarof, K.Nyuberg, P.Rogaway, B.Schneier, H.Yap илмий мақолалари, буль функцияларини криптографик асклантиришда қўлланиши ва бардошлигини баҳолашда ҳисса қўшган А.Е.Жуков, Б.В.Изотов, О.В.Логачев, А.А.Молдовян, Н.А.Молдовян, Б.В.Рязанов, А.А.Сальников, В.В.Яшенко, C.Adams, M.H.Dawson, K.Kurosawa, S.Lloyd, J.L.Massey, W.Meier, S.Mister, K.Nyberg, B.Preneel, T.Sato, J.Seberry, T.Siegentler, O.Staffelbach, S.E.Tavares, A.F.Webster каби олимларнинг илмий мақолалари ва ахборот хавфсизлигини таъминлаш йўналишида тадқиқот олиб бораётган ўзбек олимлари М.М.Арипов, П.Ф.Хасанов, С.К.Ганиев, М.М.Каримов, Д.Е.Акбаров, Х.П.Хасановларнинг илмий ишлари билан яқиндан танишиб чиқилди.

Фейстел тармоқларига асосланган кўпгина криптоалгоритмлар ахборотни криптографик ҳимоялашни етарли даражада таъминлашига қарамай, бардошлиги юқори бўлмаган криптоалгоритмлар ҳам мавжуд. Шунинг учун криптографик тизимларнинг бардошлилигини янада ошириш мақсадида Фейстел тармоғини такомиллаштириш ва янги криптоалгоритмлар ишлаб чиқиш бўйича илмий изланишлар олиб бориш ҳамиша долзарб масала бўлиб қолади.

Мавзунинг долзарблигидан келиб чиққан ҳолда диссертация ишида ахборотнинг криптографик ҳимоялаш масалаларини самарали ечиш учун Фейстел тармоғи такомиллаштирилган. Ишлаб чиқилган такомиллашган Фейстел тармоғи асосида криптоалгоритмлар яратилди.

Диссертация ишининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация иши Ўзбекистон Республикаси Президенти И.А. Каримовнинг 2007 йил 3 апрелдаги «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» ПҚ-614–сон қарорининг бажарилиши юзасидан шахсий режага мувофиқ олиб борилаётган илмий тадқиқот ишларидан бири ҳисобланади.

Тадқиқот мақсади. Фейстел тармоғини такомиллаштириш ва унга асосланган бардошли криптоалгоритмлар яратиш.

Тадқиқот вазифалари. Тадқиқот мақсадини амалга ошириш учун диссертация ишида қуйидаги вазифалар қўйилди:

-- Фейстел тармоғини тадқиқ этиш ва бу тармоққа асосланган мавжуд криптографик алгоритмлар асосий акслантиришларининг криптографик хоссаларини таҳлил этиш;

– S блок акслантиришлари яратишда уларнинг буль функция кўринишидаги моделларидан фойдаланиб, криптотаҳлил усулларига бардошлигини баҳолаш;

– Фейстел тармоғининг асосий афзалликларини сақлаб қолган ҳолда уни такомиллаштириш;

– Фейстел тармоғига асосланган мавжуд криптоалгоритмлар асосий акслантиришларини сақлаб қолган ҳолда калит ва блок узунликларини узайтириш масаласини ечиш;

– такомиллашган Фейстел тармоғига асосланган криптоалгоритмлар яратиш;

– криптоалгоритмлар учун бардошли S блок акслантиришларини яратиш.

Тадқиқот объекти ва предмети. Тадқиқот объекти сифатида криптоалгоритмлар, Фейстел тармоғи, криптоалгоритмларда қўлланилган акслантиришлар хизмат қилади.

Тадқиқот предмети сифатида функционал Фейстел тармоқлари ва бу тармоқларга асосланган шифрлаш алгоритмлари хизмат қилади.

Тадқиқот методлари. Диссертация ишида информатика ва криптология асослари, ахборот-коммуникация технологиялари ва буль функциялар хоссаларидан фойдаланилган.

Тадқиқот гипотезаси. Ахборотни криптографик ҳимоялаш масалалари учун Фейстел тармоғини такомиллаштириш, бу тармоқ асосида янги криптоалгоритмлар ишлаб чиқишга йўл очади.

Ҳимояга олиб чиқилаётган асосий ҳолатлар:

– функционал ва баланслашган функционал Фейстел тармоқлари структураси;

–Фейстел тармоғига асосланган мавжуд криптоалгоритмларни функционал ва баланслашган функционал Фейстел тармоғига ўтказиш усуллари;

– функционал Фейстел тармоғига асосланган FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2 ва баланслашган функционал Фейстел тармоғига асосланган BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 криптоалгоритмлари;

– бардошлиги юқори бўлган S блок акслантиришлари.

Илмий янгилиги қуйидагилардан иборат:

– функционал ва баланслашган функционал Фейстел тармоқлари ишлаб чиқилган;

– Фейстел тармоғига асосланган мавжуд криптоалгоритмларни функционал ва баланслашган функционал Фейстел тармоқларига ўтказиш усуллари таклиф этилган;

– функционал Фейстел тармоғига асосланган FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2 ва баланслашган функционал Фейстел тармоғига асосланган BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 криптоалгоритмлари яратилган;

– криптоалгоритмлар учун бардошли S блок акслантиришлари яратилган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Функционал ва баланслашган функционал Фейстел тармоқлари янги криптоалгоритмлар ишлаб чиқишда, мавжуд Фейстел тармоқларига асосланган криптоалгоритмларни калит ва блок узунликларини оширишда ҳамда ўқув муассаларида криптография фанидан таълим беришда қўлланилиши мумкинлиги билан илмий аҳамиятга эга.

Таклиф этилган криптоалгоритмларни аппарат воситаси нисбатан арзон тушиши ва ахборот-коммуникация тармоқларида маълумотларни муҳофазалашда қўлланилиши мумкинлиги билан амалий аҳамиятга эга.

Натижаларнинг жорий қилиниши. Тадқиқот натижаларидан FFTBSHA256–1 ва BFFTBSHA128–2 криптоалгоритмлари дастурий таъминоти «Dataprizma» МЧЖ да савдо ҳужжатларини ҳимоялашда жорий

этилган. FFTBSHA256–2 криптоалгоритми UNICON.UZ ДУК да ишлаб чиқилган «Himfayl» тизими 1-вариантида фойдаланилган.

Диссертация ишининг биринчи ва иккинчи боблари Ўзбекистон миллий университети «Механика-математика» факультети ва Тошкент давлат иқтисодиёт университети «Ахборот технологиялари ва менежмент» факультетида таълим жараёнида қўлланилган.

Ишнинг синовдан ўтиши. Диссертация натижалари «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги» республика семинарида (Тошкент ш. 2010 й.) ва Ўзбекистон алоқа ва ахборотлаштириш агентлиги «UNICON.UZ» ДУК-Фан-техника ва маркетинг тадқиқотлари марказида (Тошкент ш. 2011 й.) маъруза қилинган ва муҳокамадан ўтган.

Натижаларнинг эълон қилинганлиги. Диссертациянинг асосий мазмуни 7 та илмий ишларда акс этган, шулардан 6 таси журнал мақолалари ва 1 таси CD-дискда тарқатилган.

Диссертациянинг тузилиши ва ҳажми. Диссертация иши кириш қисми, 3 та боб, хулоса, 107 та фойдаланилган адабиётлар рўйхати ва 6 та иловадан иборат. Диссертация ишининг асосий қисми 111 варақ машина матнида ёритиб берилган ва 42 та расм ҳамда 28 та жадвалдан иборат.

Диссертация ишини тайёрлашда ўз тажрибалари ва илмий маслаҳатлари билан кўмак берган илмий раҳбарим физика-математика фанлари доктори, профессор М.М.Ариповга ҳамда услубий маслаҳатлар берган техника фанлари номзоди О.П.Ахмедовага ўз миннатдорчилигимни билдираман.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация иши мавзусининг долзарблиги, муаммонинг ўрганилганлик даражаси, тадқиқот объекти ва предмети, тадқиқотнинг мақсади ва вазифалари аниқланиб, асослаб берилди. Илмий ишни бажаришда фойдаланилган тадқиқот методлари, тадқиқотнинг илмий янгилиги, тадқиқот натижаларининг илмий ва амалий аҳамияти, ҳимояга олиб чиқилаётган асосий илмий ҳолатлар, ишнинг синовдан ўтганлиги, натижаларнинг эълон қилинганлиги, диссертация ишининг тузилиши ва ҳажми тўғрисидаги ахборотлар баён этилган.

Диссертация ишининг **биринчи бобида** Фейстел тармоғи, афзалликлари, аппарат таъминоти схемаси, қўлланиладиган асосий операторлар, криптоалгоритм S блоклари бардошлигини баҳолашда қўлланиладиган буль функцияларнинг асосий хоссалари ёритиб берилган.

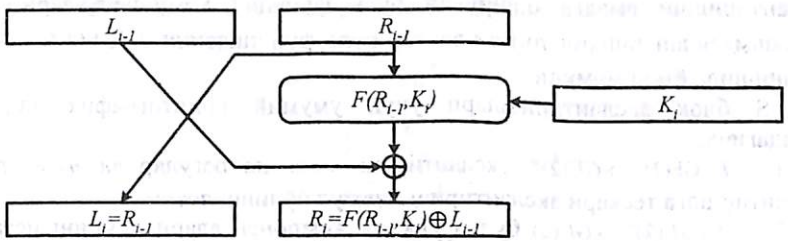
Ахборот технологиялари ривожланиб бориши билан ахборотни ҳимоялаш масаласи ҳам долзарб масалалардан бири бўлиб қолди. 1970 йиллар бошида IBM компанияси ахборот хавфсизлиги бўйича илмий тадқиқотларини олиб боришга киришди. Тадқиқотчилар гуруҳига Хорст

Фейстел бошчилик қилди. Тадқиқотлар натижасида янги бир томонли акслантиришлар асосида симметрик криптоалгоритм архитектураси яратилди. Яратилган архитектура адабиётларда Фейстел архитектураси ёки тармоғи деб номланади. n-раундли тармоқнинг шифрлаш ва дешифрлаш акслантиришларини қуйидаги формулалар орқали ифода этиш мумкин:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), i = \overline{1...n} \end{cases} \quad (1) \qquad \begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), i = \overline{n...1} \end{cases} \quad (2)$$

бу ерда L_{i-1}-чап ярим блок, R_{i-1}-ўнг ярим блок, F-раунд функцияси ва K_i-раунд калити.

Фейстел тармоғининг i-раунди 1-расмда келтирилган.



1-расм. Фейстел тармоғи i-раунди

1–расмдан кўриниб турибдики, Фейстел тармоғининг битта раундида блокнинг ярми ўзгаради, чунки $R_{i-1} = L_i$.

Фейстел тармоғи акслантиришларининг асосий хоссаси шундан иборатки, F раунд функцияси қайтмас бўлса ҳам, Фейстел тармоғи бу акслантиришларини қайтариб беради. Фейстел тармоғининг ушбу хоссаси шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиш имконини беради. Бу эса ўз навбатида тармоқ аппарат таъминоти воситаси қуришда қулайлик яратади, яъни битта аппарат воситадан шифрлашда ва дешифрлашда фойдаланиш мумкин.

Фейстел тармоғига асосланган криптоалгоритмларнинг амалиётда қўллаш афзалликлари қуйидагилардан иборат:

- шифрлашда ва дешифрлашда битта аппарат воситадан фойдаланиш имконини беради, фақат калитлар жойлашиш тартиби ўзгаради;
- криптоалгоритм итератив бўлгани учун, битта раунд учун микросхема ясаб, микросхемадан чиққан қийматни яна шу микросхема киришига бериш имконини беради;
- криптоалгоритм аппарат воситаси нисбатан арзонга тушади.

Х.Фейстел томонидан яратилган тармоқдан ташқари бу тармоқ асосида яратилган бир неча тармоқлар мавжуд. Х.Фейстел, Б.Шнайер томонидан яратилган тармоқ ва баланслашмаган Фейстел тармоғи раунд функциялари сони битта, ярим блоклар сони эса иккитага тенг бўлса, кенгайтирилган Фейстел тармоғи ва регистрларга асосланган умумлашган Фейстел тармоғи

раунд функциялари сони битта, ярим блоклар сони эса m га тенг. Худди шунингдек, умумлашган Фейстел тармоғи раунд функциялари сони m га, ярим блоклар сони $2m$ га бўлса, биринчи, иккинчи, учинчи типдаги такомиллашган Фейстел тармоғи раунд функциялари мос равишда битта, иккита, учта бўлиб, ярим блоклар сони тўртга тенг.

Симметрик блокли шифрлаш алгоритмлар бардошлилиги бу шифрлаш алгоритмида қўлланилган S блокнинг бардошлилигига узвий боғлиқ. S блокнинг бардошлилигини эса буль функциялари хоссалари орқали баҳоланади. Ҳар қандай S блокни $GF(2)^n$ фазодаги n-ўлчовли вектор $X=(x_1,x_2,...,x_n)$ ни $GF(2)^m$ фазодаги m-ўлчовли $Y=(y_1,y_2,...,y_m)$ векторга акслантириш сифатида қараш мумкин. Бу турдаги $GF(2)^n \to GF(2)$ акслантиришни амалга оширувчи буль функция компоненталари $f_i(X)$ бирлашмасидан ташкил топган вектор буль функциясини $F: GF(2)^n \to GF(2)^m$ кўринишида ёзиш мумкин.

S блок акслантиришлари учун умумий криптографик талаблар қуйидагича:

1. $F: \mathrm{GF}(2)^n \to GF(2)^m$ акслантириш $n \geq m$ да регуляр ва $n=m$ да бу акслантиришга тескари акслантириш мавжуд бўлиши лозим.
2. $f_i: GF(2)^n \to GF(2)$ буль функция компоненталари ва унинг исталган чизиқли комбинациялари баланслашган бўлиши лозим.
3. Буль функция компоненталари алгебраик чизиқсизлик даражаси $\deg(f)$ юқори бўлиши лозим.
4. Буль функция компоненталари чизиқсизлиги $NL(f)$ юқори бўлиши лозим.
5. $F(X)$ акслантириши чизиқсизлиги $NL(\varphi(X))$ юқори ёки вектор буль функция ўртача чизиқсизлиги $\overline{NL}(F)$ юқори бўлиши лозим.
6. $D^F=(\Delta^F_{a\to b})$ дифференциал матрица қийматлари катта бўлмаслиги лозим. Идеал ҳолатда матрица элементлари 0 ва 2 қийматларни қабул қилади.
7. $C^F=(c^F_{u,v})_{u,v}$ корреляцион матрица қийматлари катта бўлмаслиги лозим.
8. S блок акслантириши максимал тартибли SAC ни қаноатлантириши лозим.
9. S блок акслантириши максимал тартибли BIC ни қаноатлантириши лозим.

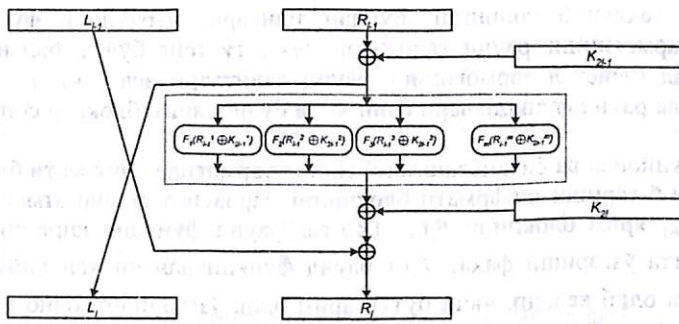
Келтирилган талаблардан 7 шарт чизиқли криптотаҳлил усулига, 6 шарт дифференциал криптотаҳлил усулига, 1-2 шарт эса танланган S блокнинг статистик криптотаҳлил усулига нисбатан бардошлигини баҳолашда қўлланилади. 8-9 шарт эса калит ёки очиқ матннинг битта бити ўзгаришига шифрматннинг тўлиқ ўзгаришини таъминлайди. Аммо, бу шартларнинг ҳаммаси бир вақтнинг ўзида бажарилмайди. Шунинг учун алгоритм S

блокларини шундай танлаш керакки, бу S блоклар бир вақтнинг ўзида мавжуд криптотаҳлил усулларига нисбатан бардошли бўлиши лозим.

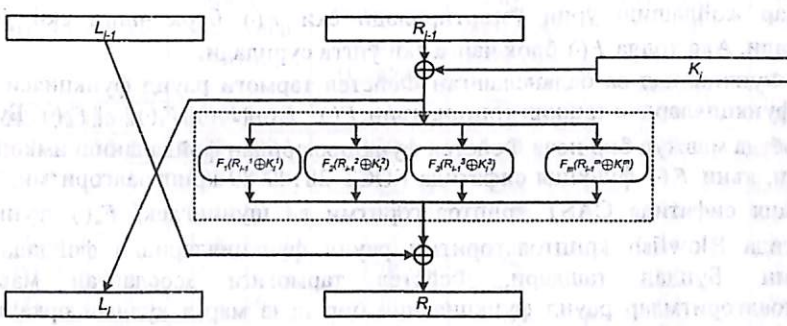
Иккинчи бобда Фейстел тармоғининг такомиллашган кўриниши бўлган функционал ва баланслашган функционал Фейстел тармоқлари таклиф этилган, бу тармокларнинг афзалликлари, аппарат воситалари функционал схемаси, Фейстел тармоғига асосланган мавжуд криптоалгоритмларни функционал ва баланслашган функционал Фейстел тармоқларига ўтказиш усуллари таклиф этилган.

Функционал ва баланслашган функционал Фейстел тармоғининг блок узунлиги 2^l $(l > 6, l \in N)$ битга тенг ва раунд калитлари узунлиги 2^{l-1} бит бўлиб, раунд функцияси бир неча функциялардан ташкил топган.

Таклиф этилган функционал ва баланслашган функционал Фейстел тармоқларининг i–раунди схемалари 2 ва 3–расмда келтирилган.



2–расм. Функционал Фейстел тармоғи *i*–раунди схемаси



3–расм. Баланслашган функционал Фейстел тармоғи *i*–раунди схемаси

n–раундли функционал ва баланслашган функционал тармоқлар шифрлаш ва дешифрлаш формулалари (3)–(6) да келтирилган.

$$\begin{cases} L_i = R_{i-1} \oplus K_{2i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1} \oplus K_{2i-1}) \oplus K_{2i}, \ i = \overline{1...n}; \\ R_{n+1} = R_n \oplus K_{2n+1}, \\ L_{n+1} = L_n \oplus K_{2n+2}; \end{cases} \quad (3)$$

$$\begin{cases} R_{i-1} = L_i \oplus K_{2i}, \\ L_{i-1} = R_i \oplus F(L_i \oplus K_{2i}) \oplus K_{2i-1}, \ i = \overline{n+1...2}; \\ L_0 = L_1 \oplus K_2, \\ R_0 = R_1 \oplus K_1; \end{cases} \quad (4)$$

$$\begin{cases} L_i = R_{i-1} \oplus K_i, \\ R_i = L_{i-1} \oplus F(R_{i-1} \oplus K_i), i = \overline{1...n}; \\ R_{n+1} = R_n \oplus K_{n+1}, \\ L_{n+1} = L_n \oplus K_{n+2}; \end{cases} \quad (5)$$

$$\begin{cases} R_{i-1} = L_i \oplus K_{i+1}, \\ L_{i-1} = R_i \oplus F(L_i \oplus K_{i+1}), i = \overline{n+1...2}; \\ L_0 = L_1 \oplus K_2, \\ R_0 = R_1 \oplus K_1; \end{cases} \quad (6)$$

(3), (4), (5) ва (6) формулаларда, функционал ва баланслашган функционал Фейстел тармоғида шифрматнни дешифрлашда шифрлаш раунд калитлари тескари тартибда қўлланилади, яъни Фейстел тармоғининг асосий афзаллиги сақланиб қолинган. Бундан ташқари, n-раундли функционал Фейстел тармоғининг раунд калитлари $2n+2$ га тенг бўлса, баланслашган функционал Фейстел тармоғининг раунд калитлари эса $n+2$ га тенг. Бу тармоқларда раунд функциялари сони m та бўлиб, ярим блоклар сони иккига тенг.

Функционал ва баланслашган Фейстел тармоғида очиқ матн блокининг битта бити ўзгариши шифрматн блокининг барчасига таъсир этмайди, яъни L_{i-1} ёки R_{i-1} ярим блокнинг $F_j(\cdot)$, $1 \le j \le m$ раунд функция киришига тўғри келган битта ўзгариши фақат $F_j(\cdot)$ раунд функциядан чиққан қийматларни ўзгаришига олиб келади, яъни бутун ярим блок ўзгаришига олиб келмайди. Агар $F_1(\cdot)$, $F_2(\cdot)$, $F_3(\cdot)$,..., $F_m(\cdot)$ раунд функциялардан чиққан блоклар узунлиги ўзаро тенг бўлса, $F(\cdot)$ раунд акслантиришидан сўнг, $F_1(\cdot)$, $F_2(\cdot)$, $F_3(\cdot)$,..., $F_n(\cdot)$ блоклар жойлашиш ўрни ўзгартирилади ёки $F(\cdot)$ блок чапга ёки ўнгга сурилади. Акс ҳолда $F(\cdot)$ блок чапга ёки ўнгга сурилади.

Функционал ва баланслашган Фейстел тармоғи раунд функцияси бир неча функциялардан ташкил топган, яъни $F(\cdot) = F_1(\cdot) \| F_2(\cdot) \| F_3(\cdot) \| ... \| F_m(\cdot)$. Бу эса амалиётда мавжуд бир неча Фейстел функцияларидан фойдаланиш имконини беради, яъни $F_1(\cdot)$ функция сифатида ГОСТ 28147-89 криптоалгоритми, $F_2(\cdot)$ функция сифатида CAST криптоалгоритми ва шунингдек, $F_m(\cdot)$ функция сифатида Blowfish криптоалгоритми раунд функцияларидан фойдаланиш мумкин. Бундан ташқари, Фейстел тармоғига асосланган мавжуд криптоалгоритмлар раунд функциясини бир неча марта қўллаш орқали бу криптоалгоритмни функционал ва баланслашган функционал Фейстел тармоғига ўтказиб, блок ва калит узунлигини ошириш мумкин. Бу ҳолатда функционал ва баланслашган функционал Фейстел тармоғи раунд функциялари бир хил бўлада, яъни $F_1(\cdot) = F_2(\cdot) = ... = = F_m(\cdot)$.

Фейстел тармоғига асосланган мавжуд криптоалгоритмларни функционал ва баланслашган функционал Фейстел тармоғига ўтказишда бу

тармоқ раунд функцияси сифатида мавжуд Фейстел тармоғи раунд функциясининг ярим блокини калитга қўшишдан сўнгги акслантиришларни олиш мумкин. Бу усулда функционал Фейстел тармоғи K_{2i-1} раунд калити $K1\|K2\|...\|Km$ калитдан, K_{2i} раунд калити эса $K1'\|K2'\|...\|Km'$ калитдан ташкил топган бўлса, баланслашган функционал Фейстел тармоғи K_i раунд калити $K1\|K2\|...\|Km$ калитдан ташкил топган, бу ерда $K1, K2,..., Km$ ва $K1', K2',..., Km'$ калитлар мавжуд Фейстел тармоғига асосланган криптоалгоритмлар раунд калитлари бўлиб, алгоритмда кўрсатилган қоида асосида генерация қилинади.

Функционал ва баланслашган функционал Фейстел тармоқлари Х.Фейстел томонидан яратилган тармоқнинг барча афзалликларини сақлаб қолган ва битта раундда L_{i-1} ёки R_{i-1} ярим блокнинг ўзгариши L_i ва R_i блокларнинг ўзгаришига олиб келади.

Учинчи бобда функционал ва баланслашган функционал Фейстел тармокларига асосланган FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2, ва BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 криптоалгоритмлари яратилган, математик модели ва S блоклари бардошлик даражалари келтирилган.

Таклиф этилган функционал ва баланслашган функционал Фейстел тармоғига асосланган барча криптоалгоритмларни асосий параметрларини 1–жадвалда умумлаштириб келтирилган.

1–жадвал

Криптоалгоритмларни асосий параметрлари

Криптоалгоритм	Калит узунлиги (битда)	Калит ўзгариш қадами (битда)	Раунд функция-лари сони	Раунд функция-лари блок узунлиги (битда)	S блоклар ўлчами ва сони
FFTBSHA256-1	128–1024	128	2	64	8x16, 4
FFTBSHA256-2	128–1024	128	4	32	8x32, 4
FFTBSHA128-1	128–1024	128	2	32	8x8, 2
FFTBSHA128-2	128–1024	128	2	32	8x8, 2
BFFTBSHA256-1	128–1024	128	4	32	8x16, 2
BFFTBSHA256-2	128–1024	128	2	64	8x8, 4
BFFTBSHA128-1	128–1024	128	1	64	8x32, 4
BFFTBSHA128-2	128–1024	128	2	32	8x8, 2

Криптоалгоритмлар раунд функциясида ҳар бир функциядан чиққан блок Р бит чапга ёки ўнгга сурилади. Сўнгра $F_1(\cdot)$, $F_2(\cdot)$, $F_3(\cdot)$,..., $F_m(\cdot)$ блоклар жойлашиш ўрнини ўзгартириш ёки блокларни бирлаштириб

$F(\cdot)=F_1(\cdot)\|F_2(\cdot)|F_3(\cdot)\|...\|F_m(\cdot)$ блокни Q бит чапга ёки ўнгга суриш мумкин. Суриш қийматлари 2–жадвалда келтирилган.

2–жадвал

Криптоалгоритмларни суриш жадвали

Раундлар сони	FFTBSHA256-1 криптоалгоритми		FFTBSHA256-2 криптоалгоритми		FFTBSHA128-1 криптоалгоритми		FFTBSHA128-2 криптоалгоритми		BFFTBSHA256-1 криптоалгоритми		BFFTBSHA256-2 криптоалгоритми		BFFTBSHA128-1 криптоалгоритми	BFFTBSHA128-2 криптоалгоритми	
	P (чапга)	Q (чапга)	P (чапга)	Q (чапга)	P (ўнгга)	Q (чапга)	P (чапга)	Q (чапга)	P (чапга)	Q (чапга)	P (чапга)	Q (чапга)	Q (ўнгга)	P (ўнгга)	Q (ўнгга)
8	8	8	4	16	4	12	4	4	4	16	8	8	8	4	4
16	4	4	2	8	2	6	2	2	2	8	4	4	4	2	2
32	2	2	1	4	1	3	1	1	1	4	2	2	2	1	1

FFTBSHA256–1 криптоалгоритмининг $F_1(R_{i-1}^1 \oplus K_{2i-1}^1)$ раунд функциясини қуйидагича ифодалаш мумкин:

$B_0=(S_0(A_0)\oplus S_1(A_5))+(S_2(A_2)\oplus S_3(A_7))$,

$B_1=(S_1(A_1)\oplus S_0(A_4))+(S_3(A_3)\oplus S_2(A_6))$,

$B_2=(S_3(A_7)\oplus S_0(A_4)\oplus S_2(A_2))+(S_2(A_6)\oplus S_0(A_0)\oplus S_1(A_5))$,

$B_3=(S_1(A_5)\oplus S_1(A_1)\oplus S_0(A_4))+(S_3(A_7)\oplus S_3(A_3)\oplus S_2(A_6))$,

$C=(B_0\|B_1\|B_2\|B_3)<<P$,

бу ерда B_0,B_1,B_2,B_3–16 битли блоклар, $C-F_1(R_{i-1}^1\oplus K_{2i-1}^1)$ раунд функциясининг 64 битли чиқувчи блоки, $A_0,A_1,A_2,A_3,A_4,A_5,A_6,A_7-F_1(R_{i-1}^1\oplus K_{2i-1}^1)$ раунд функциясига кирувчи 8 битли блоклар, P–суриш қиймати ва $R_{i-1}^1\oplus K_{2i-1}^1=A_0\|A_1\|...\|A_7$.

$F_2(R_{i-1}^2\oplus K_{2i-1}^2)$ раунд функциясини қуйидагича:

$B_0=(S_0(A_0)\oplus S_1(A_5))+(S_2(A_2)\oplus S_3(A_7))$,

$B_1=(S_1(A_1)\oplus S_2(A_6))+(S_0(A_4)\oplus S_0(A_0)\oplus S_1(A_5))$,

$B_2=(S_3(A_3)\oplus S_0(A_4))+(S_2(A_6)\oplus S_2(A_2)\oplus S_3(A_7))$,

$B_3=(S_1(A_5)\oplus S_1(A_1)\oplus S_2(A_6))+(S_3(A_7)\oplus S_3(A_3)\oplus S_0(A_4))$, $C=(B_0\|B_1\|B_2\|B_3)<<P$,

бу ерда B_0,B_1,B_2,B_3–16 битли блоклар, $C-F_2(R_{i-1}^2\oplus K_{2i-1}^2)$ раунд функциясининг 64 битли чиқувчи блоки, $A_0,A_1,A_2,A_3,A_4,A_5,A_6,A_7-F_2(R_{i-1}^2\oplus K_{2i-1}^2)$ раунд функциясига кирувчи 8 битли блоклар, P–суриш қиймати ва $R_{i-1}^1\oplus K_{2i-1}^1=A_0\|A_1\|...\|A_7$.

FFTBSHA128–1 криптоалгоритмининг $F_1(R_{i-1}^1 \oplus K_{2i-1}^1)$ раунд функциясини қуйидагича ифодалаш мумкин:

$B_0 = S_1((S_0(A_0) \oplus S_0(A_1))) \oplus S_1((S_0(A_2) \oplus S_0(A_3)))$,

$B_1 = S_1((S_0(A_1) \oplus S_0(A_2))) \oplus S_1((S_0(A_3) \oplus S_0(A_0))$,

$B_2 = S_1((S_0(A_2) \oplus S_0(A_3))) \oplus B_1$, $B_3 = S_1((S_0(A_0) \oplus S_0(A_1)) \oplus B_0$,

$C = (B_0 \| B_1 \| B_2 \| B_3) >> P$,

бу ерда $C - F_1(R_{i-1}^1 \oplus K_{2i-1}^1)$ раунд функциясининг 32 битли чиқувчи блоки, B_0, B_1, B_2, B_3–8 битли блоклар, $A_0, A_1, A_2, A_3 - F_1(R_{i-1}^1 \oplus K_{2i-1}^1)$ раунд функцияга кирувчи 8 битли блоклар, P–суриш қиймати ва $R_{i-1}^1 \oplus K_{2i-1}^1 = A_0 \| A_1 \| A_2 \| A_3$.

$F_2(R_{i-1}^2 \oplus K_{2i-1}^2)$ раунд функциясини математик модели қуйидагича:

$B_0 = S_1((S_0(A_0) \oplus S_0(A_2))) \oplus S_1((S_0(A_1) \oplus S_0(A_3)))$,

$B_1 = S_1((S_0(A_0) \oplus S_0(A_3))) \oplus S_1((S_0(A_1) \oplus S_0(A_2))$,

$B_2 = S_1((S_0(A_1) \oplus S_0(A_3))) \oplus B_0$, $B_3 = S_1((S_0(A_0) \oplus S_0(A_2)) \oplus B_1$,

$C = (B_0 \| B_1 \| B_2 \| B_3) >> P$,

бу ерда $C - F_2(R_{i-1}^2 \oplus K_{2i-1}^2)$ раунд функциясининг 32 битли чиқувчи блоки, B_0, B_1, B_2, B_3–8 битли блоклар, $A_0, A_1, A_2, A_3 - F_2(R_{i-1}^2 \oplus K_{2i-1}^2)$ раунд функцияга кирувчи 8 битли блоклар, P–суриш қиймати ва $R_{i-1}^2 \oplus K_{2i-1}^2 = A_0 \| A_1 \| A_2 \| A_3$.

BFFTBSHA256–2 криптоалгоритми $F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функцияси қуйидагича ифодалаш мумкин:

$B_0 = (S_0(A_0) \oplus S_1(A_5)) + B_1$, $B_1 = (S_1(A_1) + (S_3(A_3) \oplus S_0(A_4))) \oplus (S_2(A_2) \oplus S_3(A_7))$,

$B_2 = (S_2(A_2) \oplus S_3(A_7)) + B_3$, $B_3 = (S_3(A_3) + (S_1(A_1) \oplus S_2(A_6))) \oplus (S_0(A_0) \oplus S_1(A_5))$,

$B_4 = (S_0(A_4) \oplus S_3(A_3)) + B_7$, $B_5 = S_1(A_5) + (S_2(A_2) \oplus S_3(A_7)) \oplus (S_3(A_3) \oplus S_0(A_4))$,

$B_6 = (S_2(A_6) \oplus S_1(A_1)) + B_5$, $B_7 = (S_3(A_7) + (S_0(A_0) \oplus S_1(A_5))) \oplus (S_1(A_1) \oplus S_2(A_6))$,

$C = (B_0 \| B_1 \| B_2 \| B_3 \| B_4 \| B_5 \| B_6 \| B_7) << P$.

бу ерда $C - F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функциясининг 64 битли чиқувчи блоки, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7–8 битли блоклар, $A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7 - F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функцияга кирувчи 8 битли блоклар, P–суриш қиймати ва $R_{i-1}^1 \oplus K_i^1 = A_0 \| A_1 \| ... \| A_7$.

$F_2(R_{i-1}^2 \oplus K_i^2)$ раунд функцияси қуйидагича ифодаланади:

$B_0 = (S_0(A_0) \oplus (S_3(A_7) + S_2(A_2))) + (S_1(A_5) + S_2(A_6))$, $B_1 = (S_1(A_1) + S_0(A_0)) + B_4$,

$B_2 = (S_2(A_2) \oplus (S_1(A_1) + S_0(A_0))) + (S_3(A_3) + S_0(A_4))$, $B_3 = (S_3(A_3) + S_0(A_4)) + B_0$,

$B_4 = (S_0(A_4) \oplus (S_1(A_5) + S_2(A_6))) + (S_2(A_2) + S_3(A_7))$, $B_5 = (S_1(A_5) + S_2(A_6)) + B_2$,

$B_6 = (S_2(A_6) \oplus (S_3(A_3) + S_0(A_4))) + (S_0(A_0) + S_1(A_1)))$, $B_7 = (S_3(A_7) + S_2(A_2)) + B_6$,

$C = (B_0 \| B_1 \| B_2 \| B_3 \| B_4 \| B_5 \| B_6 \| B_7) << P$,

бу ерда $C - F_2(R_{i-1}^2 \oplus K_i^2)$ раунд функциясининг 64 битли чиқувчи блоки, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7–8 битли блоклар, $A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7 - F_2(R_{i-1}^2 \oplus K_i^2)$ раунд

функцияга кирувчи 8 битли блоклар, P–суриш киймати ва $R_{i-1}^2 \oplus K_i^2 = A_0 \| A_1 \| ... \| A_7$.

BFFTBSHA128–1 криптоалгоритмининг $F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функцияси куйидагича:

$B_0 = S_0(A_0) \oplus S_0(A_4) \oplus S_3(A_3) \oplus S_3(A_7) \oplus S_1(A_5)$,

$B_1 = S_1(A_1) \oplus S_1(A_5) \oplus S_0(A_0) \oplus S_0(A_4) \oplus S_2(A_6)$,

$B_2 = S_2(A_2) \oplus S_2(A_6) \oplus S_1(A_1) \oplus S_1(A_5) \oplus S_3(A_7)$,

$B_3 = S_3(A_3) \oplus S_3(A_7) \oplus S_2(A_2) \oplus S_2(A_6) \oplus S_0(A_4)$,

$B_4 = S_2(A_2) \oplus S_2(A_6) \oplus S_0(A_4) \oplus B_0$, $B_5 = S_3(A_3) \oplus S_3(A_7) \oplus S_1(A_5) \oplus B_1$,

$B_6 = S_0(A_0) \oplus S_0(A_4) \oplus S_2(A_6) \oplus B_2$, $B_7 = S_1(A_1) \oplus S_1(A_5) \oplus S_3(A_7) \oplus B_3$,

$C_0 = ((B_0 \oplus B_1) + B_2) \oplus B_3$, $C_1 = ((B_0 \oplus B_1) \oplus B_2) + B_3$, $D = (C_0 \| C_1)$,

бу ерда $D - F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функциясининг 64 битли чиқувчи блоки, B_0, B_1, B_2, B_3, B_4, B_5, B_6, B_7, C_0, C_1–32 битли блоклар, $A_0, A_1, A_2, A_3, A_4, A_5, A_6, A_7$ – $F_1(R_{i-1}^1 \oplus K_i^1)$ раунд функцияга кирувчи 8 битли блоклар ва $R_{i-1}^1 \oplus K_i^1 = A_0 \| A_1 \| ... \| A_7$.

n–раундли FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2 криптоалгоритмларида $2n+6$ та K_i раунд калитлари қўлланилган. $K_1, K_2, ..., K_{2n+2}$ калитлар (3) формула бўйича қўлланилади. Шифрлашда очиқ матнга $K_{2n+3} \| K_{2n+4}$ калит XOR бўйича қўшилади, ҳосил бўлган блок (3) формула бўйича шифрланади, шифрлаш натижасида ҳосил бўлган блокга $K_{2n+5} \| K_{2n+6}$ калит XOR бўйича қўшилади ва шифрматн ҳосил бўлади, дешифрлашда эса аксинча. n–раундли BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA256128–1, BFFTBSHA256128–2 криптоалгоритмларида $n+6$ та K_i раунд калити қўлланилган. $K_1, K_2, ..., K_{n+2}$ калитлар (5) формула бўйича қўлланилади. Шифрлашда очиқ матнга $K_{n+3} \| K_{n+4}$ калит XOR бўйича қўшилади, ҳосил бўлган блок (5) формула бўйича шифрланади, шифрлаш натижасида ҳосил бўлган блокга $K_{n+5} \| K_{n+6}$ калит XOR бўйича қўшилади ва шифрматн ҳосил бўлади, дешифрлашда эса аксинча.

Криптоалгоритмнинг узунлиги l $(128 \le l \le 2048)$ битга тенг бўлган дастлабки K калити 32 битга тенг K_0^{32}, K_1^{32}, ..., $K_{Lenght-1}^{32}$, $Lenght = \frac{l}{32}$ бўлган бўлакларга бўлинади, бу ерда $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^{32} = \{k_0, k_1, ..., k_{31}\}$, $K_1^{32} = \{k_{32}, k_{33}, ..., k_{63}\}$, ..., $K_{Lenght-1}^{32} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ ва $K = K_0^{32} \| K_1^{32} \| ... \| K_{Lenght-1}^{32}$. Блок узунлиги 256 бит бўлган криптоалгоритмларда ҳар бир K_i раунд калити тўртта 32 битли K_{4i-4}^{32}, K_{4i-3}^{32}, K_{4i-2}^{32}, K_{4i-1}^{32} калитдан ташкил топган бўлса, блок узунлиги 128 бит бўлган криптоалгоритмларда ҳар бир K_i раунд калити иккита 32 битли K_{2i-2}^{32}, K_{2i-1}^{32} калитдан ташкил топган. Демак, FFTBSHA256–1,

FFTBSHA256–2 криптоалгоритми $T = 4 \cdot (2n+6)$ та, FFTBSHA128–1, FFTBSHA128–2 криптоалгоритми $T = 2 \cdot (2n+6)$ та, BFFTBSHA256–1, BFFTBSHA256–2 криптоалгоритми $T = 4 \cdot (n+6)$ та, BFFTBSHA256128–1, BFFTBSHA256128–2 криптоалгоритми $T = 2 \cdot (n+6)$ та 32 битли калит иштирок этади. Раунд калитлар генерация қилишда K_L сифатида $K_L = K_0^{32} \oplus K_1^{32} \oplus ... \oplus K_{Lenght-1}^{32} \oplus 0xFA0FA0AF$ олинади. K_i^{32}, $Lenght \le i \le T-1$ сифатида $K_i^{32} = S(K_{i-Lenght}^{32}) \oplus K_L$ қиймат олинади. K_0^{32} сифатида эса K_L қиймат олинади ва K_i^{32}, $1 \le i \le Lenght-1$ сифатида $K_i^{32} = S(K_{i-1}^{32}) \oplus K_L$ қиймат олинади. Ҳар бир K_i^{32} калит генерация қилингандан сўнг K_L қиймат чапга бир бит циклик сурилади.

Барча криптоалгоритмлар учун $S(K_i^{32})$ акслантириш ҳар хил. FFTBSHA256–1 криптоалгоритмида $S(K_i^{32}) = (S_0(a_i) \| S_1(b_i)) \oplus (S_2(c_i) \| S_3(d_i))$, FFTBSHA256–2 криптоалгоритмида $S(K_i^{32}) = (S_0(a_i) \oplus S_1(b_i)) \oplus (S_2(c_i) \oplus S_3(d_i))$, FFTBSHA128–1, FFTBSHA128–2 ва BFFTBSHA128–2 криптоалгоритмларида $S(K_i^{32}) = S_0(a_i) \| S_1(b_i) \| S_0(c_i) \| S_1(d_i)$, BFFTBSHA256–1 криптоалгоритмида $S(K_i^{32}) = (S_0(a_i) \| S_0(b_i)) \oplus (S_1(c_i) \| S_1(d_i))$, BFFTBSHA256–2 криптоалгоритмида $S(K_i^{32}) = (S_0(a_i) \| S_1(b_i) \| S_2(c_i) \| S_3(d_i))$, BFFTBSHA128–1 криптоалгоритмида $S(K_i^{32}) = (S_0(a_i) \oplus S_1(b_i) \oplus S_2(c_i) \oplus S_3(d_i))$, бу ерда $K_i^{32} = a_i \| b_i \| c_i \| d_i$, a_i, b_i, c_i, d_i - 8 битли блоклар ва S_0, S_1, S_2, S_3 криптоалгоритмларда қўлланилган S блоклар.

3–жадвалда эса частотаси 2.16 ГГц га тенг бўлган AMD Athlon 3000+ процессорида криптоалгоритмларнинг шифрлаш тезлиги ва ГОСТ 28147-89, AES криптоалгоритмларига нисбатан қиёсий таҳлили келтирилган.

3–жадвал

Криптоалгоритмларнинг шифрлаш тезлиги

Криптоалгоритм	8 раундли	16 раундли	32 раундли
AES (10 раундли)	≈2.3 Мбит/с		
ГОСТ 28147-89			≈1.95 Мбит/с
FFTBSHA256-1	≈11,7 Мбит/с	≈6 Мбит/с	≈3,1 Мбит/с
FFTBSHA256-2	≈11.7 Мбит/с	≈6 Мбит/с	≈3 Мбит/с
FFTBSHA128-1	≈7,4 Мбит/с	≈3.7 Мбит/с	≈1.9 Мбит/с
FFTBSHA128-2	≈8 Мбит/с	≈4 Мбит/с	≈2 Мбит/с
BFFTBSHA256-1	≈8.3 Мбит/с	≈4.3 Мбит/с	≈2,1 Мбит/с
BFFTBSHA256-2	≈11,1 Мбит/с	≈5,7 Мбит/с	≈2,8 Мбит/с
BFFTBSHA128-1	≈10,5 Мбит/с	≈5,5 Мбит/с	≈2,7 Мбит/с
BFFTBSHA128-2	≈8,3 Мбит/с	≈4,2 Мбит/с	≈2,1 Мбит/с

Криптоалгоритмлар S блок акслантириши асосий параметрларини AES криптоалгоритмига нисбатан қиёсий таҳлили 4–жадвалда келтирилган.

4–жадвал

Криптоалгоритмларни қиёсий таҳлили

№	Параметрлар	AES	FTBSHA256–1	FTBSHA256–2	FTBSHA128–1	FTBSHA128–2	BFTBSHA256–1	BFTBSHA256–2	BFTBSHA128–1	BFTBSHA128–2
1	балансланган	+	+	+	+	+	+	+	+	+
2	регуляр	+	–	–	+	+	–	+	–	+
3	$\deg(f)$	7	7	7	7	7	7	7	7	7
4	$NL(f)$	112	112	112	112	112	112	112	112	112
5	λ_φ	0.125	0.125	0.125	0.125	0.125	0.125	0.125	0.125	0.125
6	δ_F	1/64	1/128	1/128	1/64	1/64	1/128	1/64	1/128	1/64
7	SAC	8	8	8	8	8	8	8	8	8
8	BIC	8	8	8	8	8	8	8	8	8

Барча таклиф этилган криптоалгоритмларни таққосий жадвали 5–жадвалда келтирилган.

5–жадвал

Криптоалгоритмларни таққосий жадвали

№	Параметрлар	FTBSHA256–1	FTBSHA256–2	FTBSHA128–1	FTBSHA128–2	BFTBSHA256–1	BFTBSHA256–2	BFTBSHA128–1	BFTBSHA128–2
1	Шифрлаш тезлиги нисбатан юқори	+	+	–	–	–	+	+	–
2	Дифференциал криптотаҳлил усулига нисбатан бардошлиги юқори	+	+	–	–	+	–	+	–
3	Компьютер хотирасида нисбатан кам жой эгаллайди	–	–	+	+	–	–	–	+

ХУЛОСА

Мазкур диссертацияда Фейстел тармоғини такомиллаштиришга, такомиллашган тармоққа асосланган криптоалгоритмлар ишлаб чиқишга асосий эътибор қаратилди. Натижада, функционал ва балансланган

функционал Фейстел тармоғи, бу тармоққа асосланган криптоалгоритмлар яратилди. Тадқиқот ишида олинган натижалар қуйидагилардан иборат.

1. Фейстел тармоғи афзалликларини тўлиқ сақлаб қолган функционал ва баланслашган функционал Фейстел тармоғи яратилди. Функционал Фейстел тармоғида раунд калитлари сони $2n+2$ га тенг бўлса, баланслашган функционал Фейстел тармоғида $n+2$ га тенг. Бу эса раунд калитлари махфийлиги ҳисобига функционал Фейстел тармоқларига асосланган криптоалгоритмлар бардошлигини оширишга хизмат қилади.

2. Таклиф этилган функционал ва баланслашган функционал Фейстел тармоғи асосида яратилган криптоалгоритмларни телекоммуникация тармоғида қўллаш жараёнида битта аппарат воситадан фойдаланиш ҳисобига унинг аппарат воситаси нисбатан арзонга тушади.

3. Функционал ва баланслашган функционал Фейстел тармоғи раунд функцияси бир неча функциядан ташкил топганлиги ҳисобига Фейстел тармоғига асосланган мавжуд криптоалгоритмлар раунд функциясини бир неча марта қўллаш орқали криптоалгоритмни функционал ва баланслашган функционал Фейстел тармоғига ўтказиб, блок ва калит узунлигини ошириш мумкин.

4. Тадқиқот натижасида ишлаб чиқилган функционал Фейстел тармоғига асосланган FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2 ва баланслашган функционал Фейстел тармоғига асосланган BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 криптоалгоритмлар раундлар сонини 8, 16 ва 32 га, калит узунлиги 128 битдан 1024 битгача танлаб олинишга сабаб, фойдаланувчи маълумот махфийлигига, шифрлаш тезлигига боғлиқ ҳолда калит ва раундлар сонини танлаб олиш имконияти мавжуд.

5. FFTBSHA256–1, FFTBSHA256–2, BFFTBSHA256–2 ва BFFTBSHA128–1 криптоалгоритмлари шифрлаш тезлиги нисбатан юқорилиги билан ажралиб турса, FFTBSHA128–1, FFTBSHA128–2 ва BFFTBSHA128–2 криптоалгоритмларда ўлчами 8x8 бўлган иккита S блок қўлланилганлиги ҳисобига компьютер хотирасида кам жой эгаллайди.

6. Таклиф этилган криптоалгоритмлар шифрлаш тезликлари ГОСТ 28147-89 ва AES криптоалгоритмларига нисбатан таққослаш натижалари шуни кўрсатадики, 32 раундли FFTBSHA128–1 криптоалгоритмидан ташқари барча криптоалгоритмлар шифрлаш тезликлари ГОСТ 28147–89 криптоалгоритми шифрлаш тезлигидан юқори, 32 раундли FFTBSHA128–1, FFTBSHA128–2, BFFTBSHA256–1, BFFTBSHA128–2 криптоалгоритмидан ташқари барча криптоалгоритмлар шифрлаш тезликлари AES криптоалгоритми шифрлаш тезлигидан юқори ва 16 раундли FFTBSHA128–1, FFTBSHA128–2, BFFTBSHA256–1, BFFTBSHA128–2 криптоалгоритмларининг шифрлаш тезликлари AES криптоалгоритми шифрлаш тезлигидан юқори.

7. Тадқиқот натижаси шуни кўрсатадики, ўлчами 8x16, 8x32 бўлган S блоклар қўлланилган FTBSHA256–1, FTBSHA256–2, BFTBSHA256–1 ва BFTBSHA128–1 криптоалгоритмлар S блоклари дифференциал криптотаҳлил усулига нисбатан бардошлиги юқорилиги билан ажралиб туради, алгебраик чизиксизлик даражаси, чизиқсизлиги, чизиқли криптотаҳлил усулига нисбатан бардошлиги, қатъий лавин эффекти ва чиқувчи битлар боғлиқсизлиги критерийси AES криптоалгоритми S блокларидан фарқ қилмайди.

8. Ишлаб чиқилган барча криптоалгоритмларда P ва Q суриш қийматлари раундлар сонига боғлиқ ҳолда максимал сочиш ва аралашиш эффектига эга. Уларда очиқ матн ва калитнинг битта битта бити ўзгариши шифрматн ва ҳар бир раунд калитига таъсир этади.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ

1. Арипов М.М. Туйчиев Ғ.Н. Баланслашган функционал Фейстел тармоғи // Информатика ва энергетика муаммолари. –Тошкент, 2009. №4. 65–68 б.

2. Арипов М.М. Туйчиев Ғ.Н. Функционал Фейстел тармоқлари // «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги» республика семинарии. –Тошкент, 2010. 15–18 б.

3. Туйчиев Г.Н. Применение булевых функции в оценки стойкости S-блоков // Доклады Академии наук Республики Узбекистан. –Ташкент, 2010. №1. –С.24-28.

4. Туйчиев Ғ.Н. Фейстел тармоғига асосланган криптоалгоритмларни телекоммуникация тизимларида қўллаш афзалликлари ҳақида // ТошДТУ хабарлари. –Тошкент, 2009. №3–4. 28–31 б.

5. Туйчиев Ғ.Н Функционал Фейстел тармоғи // Информатика ва энергетика муаммолари. Тошкент, 2010. №1. 71–74 б.

6. Туйчиев Ғ.Н. Функционал ва баланслашган Фейстел тармоғи аппарат–техник таъминоти функционал схемаси //Ахборотқоммуникациялар: Тармоқлар–Технологиялар–Ечимлар. –Тошкент, 2010. №3. 27–30 б.

7. Туйчиев Ғ.Н. IDEA-128 // ТАТУ хабарлари. – Тошкент, 2009. №3. 25–27 б.

Келтирилган мақолаларнинг иккитаси ҳаммуаллифликда ёзилган бўлиб, функционал Фейстел тармоғи, мақола ва маърузада симметрик криптотизимларнинг қиёсий таҳлилига ва таснифига оид маълумотлар, функционал ва баланслашган Функционал Фейстел тармоқларига асосланган криптоалгоритмлар, тадқиқотнинг умумий вазифаларига оид маълумотлар муаллифга тегишлидир.

Техника фанлари номзоди илмий даражасига талабгор Туйчиев Ғулом Нумоновичнинг 05.13.19 – «Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги» ихтисослиги бўйича «Такомиллашган Фейстел тармоғи яратиш ва унинг татбиқлари» мавзусидаги диссертациясининг

РЕЗЮМЕСИ

Таянч (энг муҳим) сўзлар: ахборот хавфсизлиги, криптоалгоритм, Фейстел тармоғи, S блок, буль функциялари, функционал, баланслашган, калит, бардошлилик.

Тадқиқот объектлари: криптоалгоритмлар, Фейстел тармоғи, криптоалгоритмларда қўлланилган акслантиришлар.

Ишнинг мақсади: Фейстел тармоғини такомиллаштириш ва унга асосланган бардошли криптоалгоритмлар яратиш.

Тадқиқот методлари: информатика ва криптология асослари, ахборот-коммуникация технологиялари ва буль функцияларининг хоссалари.

Олинган натижалар ва уларнинг янгилиги: функционал ва баланслашган функционал Фейстел тармоқлари, бу тармоқларга асосланган FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2 ва BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 криптоалгоритмлари яратилди; криптоалгоритмлар учун бардош S блок акслантиришлари ишлаб чиқилди; Фейстел тармоғига асосланган мавжуд криптоалгоритмларни функционал ва баланслашган функционал Фейстел тармоқларига ўтказиш усуллари таклиф этилган.

Амалий аҳамияти: таклиф этилган криптоалгоритмларни аппарат воситасини арзонга тушиши ва ахборот-коммуникация тармоқларида маълумотларни муҳофазалашда қўлланиши мумкин.

Татбиқ этиш даражаси ва иқтисодий самарадорлиги: диссертация иши натижалардан FFTBSHA256–1 ва BFFTBSHA128–2 криптоалгоритмлари дастурий таъминоти «Dataprizma» МЧЖ да савдо ҳужжатларини ҳимоялашда, FFTBSHA256–2 криптоалгоритми «UNICON.UZ» ДУК да ишлаб чиқилган «Himfayl» тизими 1-вариантида фойдаланилган ҳамда ЎзМУ, ТДИУ да ўқув жараёнида қўлланилган.

Қўлланиш (фойдаланиш) соҳаси: диссертация иши натижалари ахборот-коммуникация тизимларида маълумотларни муҳофазасини оширишда ва олий ўқув муассасаларида криптология фанидан таълим беришда фойдаланиш мумкин.

РЕЗЮМЕ

диссертации Туйчиева Гулома Нумоновича на тему «Создание усовершенствованной сети Фейстеля и её применение» на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Ключевые слова: информационная безопасность, криптоалгоритм, сеть Фейстеля, S блок, булевы функции, функционал, сбалансированный, ключ, стойкость.

Объекты исследования: криптоалгоритмы, сеть Фейстеля, преобразования, используемые в криптоалгоритмах.

Цель работы: усовершенствование сети Фейстеля и создание на ее основе стойких криптоалгоритмов.

Методы исследования: основы информатики и криптологии, информационно-коммуникационные технологии и свойства булевых функций.

Полученные результаты и их новизна: созданы функциональные и сбалансированные функциональные сети Фейстеля, криптоалгоритмы FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2, BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 на основе этих сетей; разработаны стойкие S блок преобразования для криптоалгоритмов; предложены способы передачи существующих криптоалгоритмов на основе сети Фейстеля в функциональные и сбалансированные функциональные сети Фейстеля.

Практическая значимость: относительно низкая стоимость аппаратных средств предложенных криптоалгоритмов, и возможность их использования для защиты информации в информационно-коммуникационных сетях.

Степень внедрения и экономическая эффективность: из результатов диссертации, программное обеспечение криптоалгоритмов FFTBSHA256–1 и BFFTBSHA128–2 использовано в ООО «Dataprizma» для защиты коммерческих документов, криптоалгоритм FFTBSHA256–2 использован в 1-м варианте системы «Himfayl», разработанной в ГУП «UNICON.UZ», а также в учебном процессе НУУз, ТГЭУ.

Область применения: результаты, полученные в диссертации, могут быть применены для повышения защиты информации в информационно-коммуникационных системах и в процессах обучения в высших учебных заведениях по предмету криптологии.

RESUME

Thesis of Tuychiyev Gulom Numonovich's on the scientific degree competition of the doctor of philosophy technical sciences on specialty 05.13.19 - «Information protecting methods and systems and information security» subject: «Creating enhanced Feistel network and its implementation»

Key words: information security, cryptoalgorithms, Feistel network, S box, Boolean functions, functional, balanced, key, resistance.

Subjects of the inquire: crypto algorithms, the Feistel network, conversion used in Feistel network.

Aim of the inquire: Feistel network improving and developing of the resistant crypto algorithms based on this network.

Methods of inquire: informatics and cryptology basis, information-communication technologies, Boolean functions properties.

The results achieved and their novelty: functijonal and balanced functional Feistel networks, based on this networks FFTBSHA256–1, FFTBSHA256–2, FFTBSHA128–1, FFTBSHA128–2, BFFTBSHA256–1, BFFTBSHA256–2, BFFTBSHA128–1, BFFTBSHA128–2 cryptoalgorithms and resistant S box conversions have been created; the methods of transferring of existing crypto algorithms based on Feistel network to functional and balanced functional Feistel network were offered.

Practical importance: relative low cost of offered crypto algorithm devices and their application for information security in information-communication networks.

Degree of embed and economic effectivity: from the results of thesis, the software of crypto algorithms FFTBSHA256–1 and BFFTBSHA128–2 used in «Dataprizma» LLC for commercial documents security, FFTBSHA256–2 crypto algorithm is used in 1st version of «Himfayl» system, developed in SUE «UNICON.UZ», and in educational process in NUUz, TSEU.

Sphere of usage: results achieved in the thesis can be used in information and communication systems and in education process in institutes of higher education on cryptology subject.

Босишга рухсат этилди. 29.09.2011 й.
Босма табоқ 1,375. Адади 60. Буюртма № 29/09.
“Yosh kuch press matbuoti” МЧЖ босмахонасида чоп этилди.
Манзил: Тошкент, Сўгалли ота, 5.