ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.FM.01.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

ТУЙЧИЕВ ҒУЛОМ НУМОНОВИЧ

ЯГОНА АЛГОРИТМГА АСОСЛАНГАН ФУНКЦИОНАЛ ЛАЙ–МЕССИ ТАРМОҒИ НАЗАРИЯСИ ВА АМАЛИЁТИ

05.01.05–Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ФИЗИКА–МАТЕМАТИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент–2017

УДК: 004.056.55

Физика–математика фанлари бўйича фан доктори (DSc) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора наук (DSc) по физико–математическим наукам

Contents of dissertation abstract of doctor of science (DSc) on physico–mathematical sciences

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.FM.01.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

ТУЙЧИЕВ ҒУЛОМ НУМОНОВИЧ

ЯГОНА АЛГОРИТМГА АСОСЛАНГАН ФУНКЦИОНАЛ ЛАЙ–МЕССИ ТАРМОҒИ НАЗАРИЯСИ ВА АМАЛИЁТИ

05.01.05–Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ФИЗИКА–МАТЕМАТИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент–2017

Фан доктори (Doctor of Science) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2017.1.DSc/FM3 рақам билан рўйхатга олинган.

Диссертация Ўзбекистон Миллий университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб саҳифасида (www.nuu.uz) ва «ZIYONET» ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий маслаҳатчи:	**Арипов Мирсаид Мирсидикович** физика–математика фанлари доктори, профессор
Расмий оппонентлар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Касимов Надимулло Хабибуллаевич физика–математика фанлари доктори, профессор
	Утеулиев Ниетбай Утеулиевич физика–математика фанлари доктори, профессор
Етакчи ташкилот:	**«UNICON.UZ» ДУК**

Диссертация ҳимояси Ўзбекистон Миллий университети ҳузуридаги илмий даражалар берувчи DSc.27.06.2017.FM.01.02 рақамли илмий кенгашнинг 2017 йил «___» _____ соат 10^{00} даги мажлисида бўлиб ўтади. (Манзил: 100174, Ташкент, Талабалар шаҳарчаси, Университет–4 кўчаси. Тел.:(99871) 246–02–24; факс:(99871) 246–53–21; e–mail: info@nuu.uz).

Докторлик диссертацияси билан Ўзбекистон Миллий университети Ахборот–ресурс марказида танишиш мумкин (_____ рақами билан рўйхатга олинган). (Манзил: 100174, Ташкент, Талабалар шаҳарчаси, Университет–4 кўчаси. Тел.:(99871) 246–02–24; факс:(99871) 246–53–21; e–mail: info@nuu.uz).

Диссертация автореферати 2017 йил «____»_____ куни тарқатилди.
(2017 йил «___»_____даги _____ рақамли реестр баённомаси)

А.Р.Марахимов
Илмий даражалар берувчи
илмий кенгаш раиси, т.ф.д.

З.Р.Рахмонов
Илмий даражалар берувчи
илмий кенгаш котиби, ф.–м.ф.д.

Р.Д.Алоев
Илмий даражалар берувчи
илмий кенгаш қошидаги
илмий семинар раиси, ф.–м.ф.д.

КИРИШ (фан доктори (DSc) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда криптография ахборот хавфсизлиги соҳасида муҳим ўрин эгаллайди. «Криптографиянинг ахборотни ҳимоялашдаги аҳамияти у қўлланиладиган ва кўпчилик инсонларнинг манфаатларига дахл қиладиган соҳалар кенгайиши баробарида ошиб бормоқда»[1]. Дунё миқёсида ахборот технологияларининг жадал ривожланиши билан ахборотни ҳимоялашга бўлган эҳтиёж ортмоқда ва кенг қамровли илмий изланишлар олиб борилмоқда. Бу борада шифрлаш алгоритмлари операцион тизимларнинг ажралмас қисмига айланган ва ахборотларни узатиш, сақлаш, қайта ишлаш жараёнида кенг татбиқ этилишига талаб ортиқ бормоқда. Шу сабабли, шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқлар, тармоқ асосида шифрлаш алгоритмлари, шифрлаш алгоритмлари учун S–блоклар ишлаб чиқиш долзарб муаммолардан бири ҳисобланади. Блокли шифрлаш алгоритмлари, S–блоклар ишлаб чиқиш соҳасида жаҳонда маълум ютуқларга эришилган бўлиб, шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқ, тармоқ асосида шифрлаш алгоритмлари, бардошли S–блоклар ишлаб чиқиш, шифрлаш алгоритмларини бардошлигини баҳолаш муҳим вазифалардан бири бўлиб қолмоқда.

Мустақиллик йилларида мамлакатимизда криптография соҳасини самарали ривожланишига ҳамда бардошлиги юқори бўлган шифрлаш алгоритмларини ишлаб чиқишга алоҳида эътибор қаратилди. Бу борада, жумладан бардошлилиги юқори бўлган шифрлаш алгоритмларини ишлаб чиқиш, шифрлаш алгоритмлари асосида тузилган дастурий таъминот ва дастурий аппарат воситалари, функционал Фейстел тармоқларини яратиш, криптографик акслантиришлар бардошлилигини баҳолаш усулларини яратишга бағишланган қатор илмий–тадқиқотлар олиб борилган ва сезиларли натижаларга эришилмоқда. Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси асосида ахборот хавфсизлигини таъминлаш, ахборотни ҳимоя қилиш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга ўз вақтида муносиб қаршилик кўрсатишни таъминлаш муҳим аҳамиятга эга.

Жаҳон амалиётида шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган ва раунд функциядан ташкил топган тармоқ, бу тармоқга асосланган шифрлаш алгоритмлари ва улар учун бардошлилиги юқори бўлган S–блоклар ишлаб чиқиш алоҳида аҳамият касб этиб бормоқда. Бу борада мақсадли илмий тадқиқотлар, жумладан, қуйидагиларга алоҳида эътибор қаратилмоқда: шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқлар ва улар асосида шифрлаш алгоритмларини яратиш, шифрлаш алгоритмлари бардошлигини баҳолаш, бардошли S–блок ишлаб чиқиш каби йўналишларда мақсадли илмий изланишларни амалга ошириш муҳим вазифалардан бири ҳисобланади.

[1] Ростовцев А.Г. Алгебраическое основы криптографии, 2000 г.

Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги ПҚ–614–сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора–тадбирлари тўғрисида»ги Қарори, Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги 242–сон «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш туғрисидаги низомни тасдиқлаш ҳақидаги»ги қарори, Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ–4947–сон «Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида»га фармони ҳамда мазкур фаолиятга тегишли барча меъёрий-ҳуқуқий хужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти муайян даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланиши–нинг устувор йўналишларига боғлиқлиги. Мазкур тадқиқот республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот–коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Диссертация мавзуси бўйича хорижий илмий–тадқиқотлар шарҳи[2]. Шифрлаш ва дешифрлашда ягона алгоритмга асосланган тармоқлар ишлаб чиқиш, AES, ГОСТ 28147–89, IDEA, PES шифрлаш алгоритмларини бардошлилигини баҳолаш, S–блоклар ишлаб чиқиш ва бардошлигини баҳолаш усулини такомиллаштиришга йўналтирилган илмий изланишлар жаҳоннинг етакчи илмий марказлари ва олий таълим муассасалари, жумладан, Bar Ilan University, University of Haifa, Tel Aviv University, Weizmann Institute (Исроил), Katholieke University Leuven (Белгия), Криптография Академияси, Москва давлат университети, Жанубий федерал Университет (Россия), University of Luxembourg (Люксембург), Dian Ji University, Jiaotong University (Хитой), Swiss Federal Institute of Technology (Швейцария), Vienna Technical University (Австрия), Lyon University (Франция), University College London (Англия), University of California, Conterpane Internet Security (АҚШ), Indian Statistical Institute (Ҳиндистон), Korea University (Корея), Nanyang Technological University (Сингапур), Ўзбекистон Миллий университети, Тошкент ахборот технологиялари университети, «UNICON.UZ» ДУКда (Ўзбекистон) кенг қамровли илмий–тадқиқот ишлари олиб борилмоқда.

PES, IDEA, AES ва ГОСТ 28147–89 шифрлаш алгоритмларига криптотаҳлил усуллари қўллаш, шифрлаш ва дешифрлашда ягона алгоритмдан фойдаланиладиган тармоқлар ишлаб чиқиш, бардошли S–блоклар ишлаб чиқишга оид жаҳонда олиб борилган тадқиқотлар натижасида қатор, жумладан, қуйидаги илмий натижалар олинган: 6.5 ва 7 раундли IDEA шифрлаш алгоритмига Related key rectangle криптотаҳлил усули қўлланилган ва 7 раундли шифрлаш алгоритми учун 2^{65} очиқ матн–

[2] Диссертация мавзуси бўйича хорижий илмий-тадқиқотлар шарҳи Жанубий федерал Университет, University of Haifa, Swiss Federal Institute of Technology, Katholieke University Leuven, Indian Statistical Institute, University of California ва бошқа манбалар асосида ишлаб чиқилган

шифрматн жуфтлиги талаб этилиши аниқланган (Bar Ilan University, University of Haifa, Tel Aviv University, Исроил); 7 раундли PES шифрлаш алгоритмига дифференциал криптотаҳлил усули қўлланилган ва 2^{64} очиқ матн–шифрматн жуфтлиги талаб этилиши аниқланган (Swiss Federal Institute of Technology in Zurich, Швейцария); 7 ва 8 раундли AES–128, AES–192, AES–256 шифрлаш алгоритмига Impossible Differential криптотаҳлил усули қўлланилган ва 2^{91} дан кўп очиқ матн–шифрматн жуфтлиги талаб этилиши аниқланган (Bar Ilan University, University of Haifa, Исроил); ГОСТ 28147–89 шифрлаш алгоритмига алгебраик криптотаҳлил қўлланилган, S–блоклари учун тенгламалар олинган ва XSL усули билан ечилган, 2^{38} очиқ матн–шифрматн жуфтлиги талаб этилиши аниқланган (Жанубий федерал Университет, Россия); Фейстел тармоғи, унинг такомиллашган кўриниши, кенгайтирилган Фейстел тармоғи (IBM, Conterpane Internet Security, University of California, АҚШ), Лай–Месси схемаси ва унинг кенгайтирилган кўриниши ишлаб чиқилган (Swiss Federal Institute of Technology, Швейцария, Dian Ji University, Jiaotong University, Хитой); алгебраик чизиқсизлик даражаси ва чизиқсизлиги юқори S–блоклар генерация қилиш усуллари яратилган (Vienna Technical University, Katholieke Universite Leuven, Бельгия); чизиқсизлиги юқори буль функциялар генерация қилиш усуллари яратилган (Indian Statistical Institute, Ҳиндистон, University of Science and Technology of China, Хитой, University of Alabama, АҚШ).

Дунёда шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқлар, мазкур тармоқлар асосида шифрлаш алгоритмлари, бардошли S–блоклар ишлаб чиқиш ҳамда шифрлаш алгоритмларини бардошлигини баҳолаш бўйича қатор, жумладан, қуйидаги устивор йўналишларда тадқиқотлар олиб борилмоқда: мавжуд шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқларларни такомиллаштириш; мазкур тармоқлар асосида шифрлаш алгоритмларини ишлаб чиқиш; шифрлаш алгоритмлари учун бардошли S–блоклар генерация қилиш усулларини яратиш; шифрлаш алгоритмларни бардошлигини баҳолаш; чизиқсизлиги юқори бўлган буль функциялар генерация қилиш усулларини яратиш.

Муаммонинг ўрганилганлик даражаси. Ҳозирги вақтда шифрлаш ва дешифрлашда бита алгоритмдан фойдаланиладиган Лай–Месси схемасини таҳлил этиш, мазкур схема асосида шифрлаш алгоритмлари ишлаб чиқиш, таҳлил этиш масалалари бир қатор олимлар: E.Biham, O.Dunkellman, Z.Gong, P.Junod, N.Keller, X.Lai, J.Lee, Y.Luo, M.Macchetti, J.Massey, J.Nakahara, J.Park, B.Preneel, J.Rijmen, S.Vaudenay, J.Vandewalle, Z.Wu, A.Yun, М.Арипов, М.Бондаренко, И.Горбенко, В.Долгов, Р.Олейников, В.Руженцев ва бошқаларнинг илмий ишларида кўриб чиқилган.

AES, ГОСТ 28147–89 шифрлаш алгоритмларини таҳлил этиш, бардошлигини криптотаҳлил усулларига баҳолаш, алгебраик чизиқсизлиги юқори бўлган S–блок ва буль функциялари генерация қилиш масалалари билан боғлиқ тадқиқотлар бир қатор олимлар томонидан олиб борилган, жумладан: M.Aref, B.Bahrak, A.Canteaunt, C.Carlet, P.Charpin, J.Clark,

N.Courtois, I.Dinur, O.Dunkelman, D.Feng, N.Ferguson, C.Fontaine, H.Gilbert, G.Ivanov, J.Jacob, S.Kavut, N.Keller, J.Kelsey, J.Kim, S.Lucks, J.Lu, S.Maitra, M.Minier, W.Millan S.Nikova, N.Nikolov, K.Nyberg, B.Schneier, A.Shamir, M.Stay, P.Stanica, S.Stepney, S.Sung, D.Wagner, D.Whiting, W.Wu, M.Yusel, W.Zhang, X.Zhang, Б. Абдурахимов, Л.Бабенко, Е.Маро, В.Рудской каби олимлар томонидан тадқиқ қилинган.

Шу билан бирга шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиладиган тармоқ, бу тармоқ асосида шифрлаш алгоритмлари яратиш, бардошли S–блоклар ишлаб чиқиш бўйича етарли даражада илмий изланишлар олиб борилмаган.

Диссертация мавзусининг диссертация бажарилган олий таълим муассасасининг илмий–тадқиқот ишлари билан боғлиқлиги. Диссертация тадқиқоти Ўзбекистон Миллий университети илмий-тадқиқот ишлари режаси «Амалий математика ва информацион технологияларнинг долзарб муаммолари» (2012–2016) мавзуси лойиҳаси доирасида бажарилган.

Тадқиқотнинг мақсади Лай–Месси тармоғи, бу тармоқга асосланган янги шифрлаш алгоритмлари ишлаб чиқиш ва бардошли S–блоклар генерация қилишдан иборат.

Тадқиқотнинг вазифалари:

Лай–Месси схемаси ва IDEA, PES, AES, ГОСТ 28147–89 шифрлаш алгоритмларини, S–блокларни бардошлигини баҳолашда қўлланиладиган буль функциялар хоссаларини таҳлил этиш;

шифрлаш ва дешифрлашда ягона алгоритмдан фойдаланиладиган ва раунд функциялардан ташкил топган Лай–Месси тармоқлари яратиш;

Ниберг конструкцияси асосида бардошли 8x8, 4x4 ўлчамли S–блоклар ишлаб чиқиш;

AES ва ГОСТ 28147–89 шифрлаш алгоритмлари раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида янги шифрлаш алгоритмлари яратиш;

ишлаб чиқилган шифрлаш алгоритмлари бардошлигини баҳолаш.

Тадқиқотнинг объекти Лай–Месси тармоқлари, Ниберг конструкциясидан иборат.

Тадқиқотнинг предмети AES ва ГОСТ 28147–89 шифрлаш алгоритмлари раунд акслантиришларини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида яратилган янги шифрлаш алгоритмлари, S–блоклар ва буль функциялари ишлаб чиқиш усуллари ташкил этади.

Тадқиқот усуллари. Диссертация натижалари тизимли ва татбиқий дастурлаш, татбиқий криптография усуллари асосида олинган ва комбинаторика, математик логика, эҳтимоллар назариясидан фойдаланилган, янги шифрлаш алгоритмлари ва бардошли S–блок, буль функцияларлар ишлаб чиқиш усулларида дастурлаш технологияси қўлланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

IDEA шифрлаш алгоритми структураси ва Лай–Месси схемасидан фойдаланган ҳолда IDEAX–Y, RFWKIDEAX–Y кўринишдаги Лай–Месси

тармоқлари яратилган;

PES шифрлаш алгоритми структураси ва Лай–Месси схемасидан фойдаланган ҳолда PESX–Y, RFWKPESX–Y кўринишдаги Лай–Месси тармоқлари яратилган;

AES шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида AES–IDEAX–Y, AES–RFWKIDEAX–Y, AES–PESX–Y, AES–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилган;

ГОСТ 28147–89 шифрлаш алгоритмлари раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида GOST28147–89–IDEAX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилган;

Ниберг конструкцияси асосида бардошли 8x8, 4x4 ўлчамли S–блоклар ишлаб чиқилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y кўринишдаги Лай–Месси тармоқлари ишлаб чиқилган;

Ниберг конструкцияси асосида бардошлилиги юқори ўлчами 4x4, 8x8 бўлган S–блоклар ишлаб чиқилган ва дастурий таъминоти яратилган;

AES ва ГОСТ 28147–89 шифрлаш алгоритмлари акслантиришларини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш ҳисобига янги шифрлаш алгоритмлари ва дастурий таъминоти яратилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги ҳисоблаш экспериментлари натижаларини умумқабул қилинган мезонлар асосида қатъий таққослаш орқали исботланади ва сонли тадқиқотлар натижалари билан тасдиқланади. Барча шифрлаш алгоритмлари ва S–блок, буль функциялари ишлаб чиқиш усуллари дастурий таъминоти тузилган ва текширилган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти.

Тадқиқот натижаларининг илмий аҳамияти сифатида Лай–Месси тармоқлари, шунингдек, Ниберг конструкцияси асосида бардошли S–блок ва буль функциялари ишлаб чиқиш усули хизмат қилади.

Тадқиқотда олинган натижаларининг амалий аҳамияти AES ва ГОСТ 28147–89 шифрлаш алгоритмлари раунд акслантиришлари Лай–Месси тармоқлари раунд функцияси сифатида қўллаш ҳисобига бардошли ва тезлиги юқори бўлган янги шифрлаш алгоритмлари ахборотларни узатиш ва сақлаш жараёнида ҳимоялашда, бардошли S–блоклар эса блокли шифрлаш алгоритмлари ишлаб чиқишда кенг кўламда қўлланиши мумкин.

Тадқиқот натижаларининг жорий қилиниши. Ягона алгоритмга асосланган функционал Лай–Месси тармоғи асосида:

AES шифрлаш алгоритми раунд акслантиришларидан фойдаланилган ҳолда яратилган AES–IDEA32–4 шифрлаш алгоритми «UNICON.UZ» ДУК да «Himfayl» дастурий таъминотида маълумотларни шифрлаш орқали ҳимоялашда қўлланилган (Ахборот технологиялари ва коммуникацияларини

ривожлантириш вазирлигининг 2017 йил 29 майдаги 33–8/3256–сон маълумотномаси). AES–IDEA32–4 шифрлаш алгоритмида калит узунлиги ва раундлар сонини танлаш имконияти мавжудлиги, ихтиёрий форматдаги файлларни ҳимоялашда қўллаш шифрлаш тезлигини 17% га ошириш имконини берган;

ГОСТ 28147–89 шифрлаш алгоритми раунд акслантиришлари асосида яратилган GOST28147–89–IDEA16–2 шифрлаш алгоритмидан «UNICON.UZ» ДУК «Himfayl» тизимида ихтиёрий форматдаги файлларни хавфсизлигини таъминлаш максадида фойдаланилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2017 йил 29 майдаги 33–8/3256–сон маълумотномаси). GOST28147–89–IDEA16–2 шифрлаш алгоритмларида калит узунлиги ва раундлар сонини танлаш имконияти мавжудлиги, ихтиёрий форматдаги файлларни ҳимоялашда қўллаш шифрлаш тезлигини 21% га ошириш имконини берган.

AES–PES16–1, AES–RFWKPES16–1, AES–RFWKPES32–1, AES–RFWKIDEA32–1 шифрлаш алгоритмлари етакчи хорижий журналларда (International Journal of Network Security, vol.19, No.6, pp.899–903, Nov. 2017; International Journal of Network Security, vol.19, No.6, pp.984–994, Nov. 2017; International Journal of Network Security, vol.19, No.3, pp.413–420, May 2017; Displays, vol.49, pp.116–123, Sep. 2017) симметрик алгоритмларга асосланган криптографик моделлар яратишда қўлланилган. Илмий натижаларнинг қўлланилиши H–вектор функция характеристикаларини аниқлашга, бинар тасвирларда маълумотларни яширишга ва катта ҳажмдаги тасвирларни ҳимоялашга имкон берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари, жумладан 6 та халқаро ва 7 та республика илмий–амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилиниши. Тадқиқот мавзуси бўйича жами 50 та илмий иш чоп этилган, шулардан, Ўзбекистон Республикаси Олий аттестация комиссиясининг докторлик диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 21 та мақола (13 та республика ва 8 та хорижий журналларида) чоп этилган, ҳамда 6 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, бешта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 198 бетни ташкил этган.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида ўтказилган тадқиқотларнинг долзарблиги ва зарурати асосланган, тадқиқотнинг мақсади ва вазифалари, объект ва предметлари тавсифланган, республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, тадқиқотнинг илмий янгилиги ва амалий натижалари баён қилинган, олинган натижаларнинг илмий ва амалий аҳамияти очиб берилган, тадқиқот натижаларини амалиётга жорий қилиш, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Лай–Месси схемаси таҳлили ва Ниберг конструкцияси асосида S–блок, буль функциялари генерация қилиш»** деб номланган биринчи бобида Лай–Месси схемаси, бу схемага асосланган PES ва IDEA шифрлаш алгоритмлари таҳлил этилган, шифрлаш алгоритмларига қўлланилган криптотаҳлил усуллари натижалари келтирилган. Ниберг конструкцияси асосида S–блок ва буль функциялари генерация қилиш усуллари, янги шифрлаш алгоритмлари яратишда қўлланилган AES ва ГОСТ 28147–89 шифрлаш алгоритмлари акслантиришлари таҳлили келтирилган.

n–раундли Лай–Месси схемаси шифрлаш ва дешифрлаш жараёни 1 ва 2–расмларда келтирилган. Лай–Месси схемасида *F*–раунд функция, *H*–акслантириш ва K_0, K_1, ..., K_n раунд калитлари бўлсин. Очиқ матн блоки L_0 ва R_0 қисмларга бўлинади. Ҳар бир раундда қуйидагича акслантиришлар амалга оширилади:

$$(L'_{i+1}, R'_{i+1}) = H(L'_i + T_i, R'_i + T_i),$$

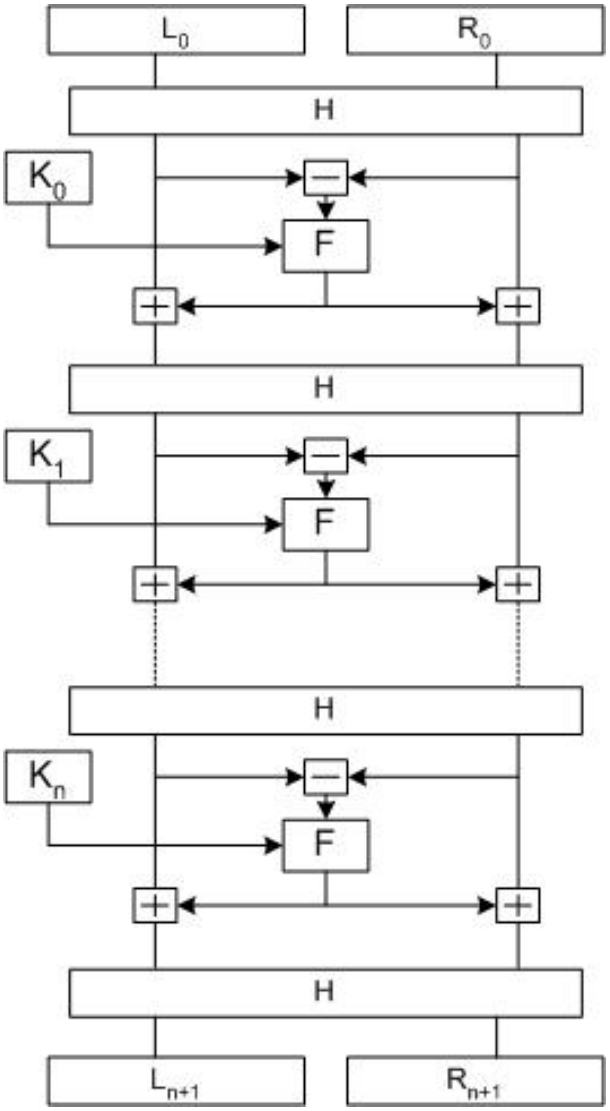
бу ерда $T_i = F(L'_i - R'_i, K_i)$ ва $(L'_i, R'_i) = H(L_0, R_0)$. Шифрматн сифатида $(L_{n+1}, R_{n+1}) = (L'_{n+1}, R'_{n+1})$ қийматлар олинади.

Фейстел тармоғи ва Лай–Месси схемасида шифрлаш қуйидагича амалга оширилади:

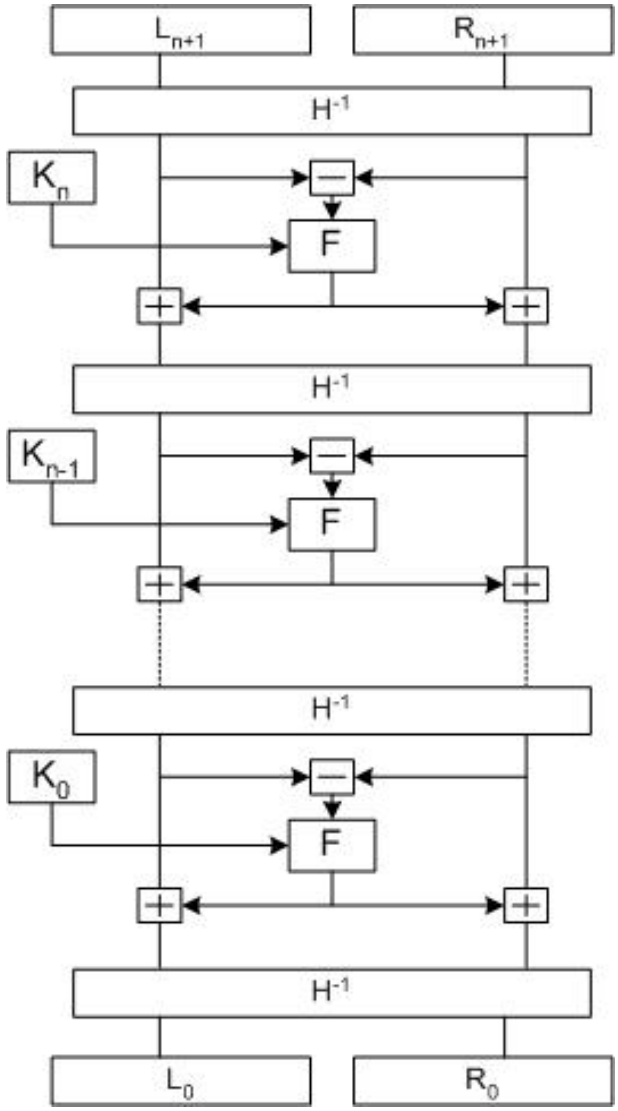
Фейстел тармоғи	Лай–Месси схемаси
1. $L_0 \leftarrow x_L$, $R_0 \leftarrow x_L$,	1. $\alpha_0 \leftarrow x_L$, $\beta_0 \leftarrow x_L$,
2. $L_{i+1} \leftarrow R_i$, $R_{i+1} \leftarrow L_i \oplus F(R_i)$,	2. $\alpha_{i+1} \leftarrow \alpha_i + F(\alpha_i - b_i)$, $\beta_{i+1} \leftarrow \beta_i + F(\alpha_i - \beta_i)$,
3. $y_L \leftarrow L_n$, $y_R \leftarrow R_n$.	3. $y_L \leftarrow \alpha_n$, $y_R \leftarrow \beta_n$.

Лай–Месси схемасида Фейстел тармоғи каби шифрлаш ва дешифрлашда битта алгоритмдан фойдаланилади, фақат раунд калитлари тескари тартибда қўлланилади ва H^{-1} акслантиришни ҳисоблаш талаб этилади.

Лай–Месси схемаси псевдохаотик (pseudorandomness) бўлиш учун учта, кучли псевдохаотик бўлиши учун тўртта раунд етарли. Демак, псевдотасодифий функциядан псевдотасодифий ўрин алмаштириш қуриш учун уч раундли, кучли псевдотасодифий ўрин алмаштириш қуриш учун тўрт раундли Лай–Месси схемаси етарли.



1–расм. *n*–раундли Лай–Месси схемаси шифрлаш жараёни



2–расм. *n*–раундли Лай–Месси схемаси дешифрлаш жараёни

PES (Proposed Encryption Standard) шифрлаш алгоритми 1991 йилда С. Лай (X. Lai) ва Ж. Месси (J. Massey) томонидан яратилган бўлиб, Лай–Месси схемасига асосланган. Шифрлаш алгоритми калит узунлиги 128 бит ва блок узунлиги 64 битга тенг, 8 раунд ва чиқувчи акслантиришдан иборат. 7 раундли PES алгоритмига дифференциал криптотаҳлил усули қўлланилди, шифрни очиш учун 2^{64} та очиқ матн–шифрматн жуфтлиги талаб этилиши маълум бўлди. Сўнгра PES шифрлаш алгоритми қайта ишлаб чиқилди ва IPES (Improved PES) деб номланди. 1992 йилда IPES шифрлаш алгоритми IDEA (International Data Encryption Algorithm) деб номланди. Алгоритм калит узунлиги 128 бит ва блок узунлиги 64 битга тенг, 8 раунд ва чиқувчи акслантиришдан иборат. Шифрлаш алгоритмларига бир неча криптотаҳлил усуллари қўлланилган бўлиб, натижалари 1 ва 2–жадвалда келтирилган.

1–жадвал

PES алгоритмига қўлланилган криптотаҳлул усуллари натижалари

Ҳужум тури	Раундлар сони	Танлаб олинган матнлар сони	Сарфланган вақт (амаллар сони)
Differential	7	2^{64}	2^{160}
SQUARE	2.5	2^{17}	2^{47}
SQUARE	2.5	2^{32}	2^{63}
Related–Key SQUARE	2.5	2	2^{41}

2–жадвал

IDEA шифрлаш алгоритмига қўлланилган ҳужум натижалари

Ҳужум тури	Раундлар сони	Танлаб олинган матнлар сони	Сарфланган вақт (амаллар сони)
Differential	2.5	2^{10}	2^{106}
SQUARE	2.5	2^{48}	2^{79}
Differential–Linear	3	2^{30}	2^{44}
Differential	3	2^{30}	$0.75 * 2^{44}$
Truncated Differential	3.5	2^{56}	2^{67}
Miss–in–the–middle	4	2^{37}	2^{70}
Related–Key Differential–Linear	4	$2^{38.3}$	–
Miss–in–the–Middle	4.5	2^{64}	2^{112}
Meet–in–the–middle	5	2^{24}	2^{126}
Linear	5	2^{19}	2^{103}
Higher–order Differential–Linear	5.5	2^{32}	2^{114}
Higher–order Differential–Linear	6	2^{64}–2^{52}	$2^{126.85}$
Related key rectangle	7	2^{65}	$2^{104.2}$

AES шифрлаш алгоритми S–блоклари Ниберг конструкцияси асосида ишлаб чиқилган. Ниберг конструкцияси эса $GF(2^k)$ Галуа майдонида $b = A \cdot y + a, \quad a,b \in GF(2^k)$ аффин акслантириш билан комбинациялашган $y = x^{-1} \bmod[f(z), p], \quad x,y \in GF(2^k)$ кўринишдаги мультипликатив тескари элементлар кўринишдаги акслантиришни ифодалайди, бу ерда $f(z) = z^8 + z^4 + z^2 + z + 1$–*GF(2)* да келтирилмайдиган кўпҳад, A–$k \times k$ ўлчамли нолга тенг бўлмаган матрица, *a*–суриш вектори, *p*–кенгайтирилган Галуа майдони 2–характеристикаси ва 0^{-1}=0 каби қабул қилинган.

Ўлчами 8x8 бўлган S–блокларини генерация қилиш учун Ниберг конструкцияси *GenerSBox(m,b)* кўринишдаги қуйидагича умумлаштирилган:

$$\begin{pmatrix} s_7 \\ s_6 \\ s_5 \\ s_4 \\ s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 \\ m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 \\ m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 \end{pmatrix} \begin{pmatrix} c_7 \\ c_6 \\ c_5 \\ c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \oplus \begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

бу erда $b=(b_0,b_1,b_2,b_3,b_4,b_5,b_6,b_7)$, $m=(m_0,m_1,m_2,m_3,m_4,m_5,m_6,m_7)$, $s=(s_0,s_1,s_2,s_3,s_4,s_5,s_6,s_7)$, $c=(c_0,c_1,c_2,c_3,c_4,c_5,c_6,c_7)$ ва a–акслантиришга кирувчи қиймат, s–акслантиришдан чиқувчи қиймат, $c=a^{-1}$. Агарда m, b b–константа ва a қиймат нолдан 255 гача ўзгарса, у ҳолда ўлчами 8x8 бўлган S–блок ҳосил бўлади, яъни $S_{8x8}=GenerSBox(m,b)$. AES шифрлаш алгоритми S–блоки сифатида $GenerSBox(241,99)$ акслантириш олинган. Алгоритм S–блоклари учун $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, $Dd_j(S)=8$, $1\le j\le 8$ шарт бажарилади.

Ўлчами 4x4 бўлган S–блокларни генерация қилиш учун Ниберг конструкцияси $GenerSBox(m^0,m^1,m^2,m^3,b)$ кўринишда кўринишда қуйидагича умумлаштирилган:

$$\begin{pmatrix} s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} m_0^0 & m_1^0 & m_2^0 & m_3^0 \\ m_0^1 & m_1^1 & m_2^1 & m_3^1 \\ m_0^2 & m_1^2 & m_2^2 & m_3^2 \\ m_0^3 & m_1^3 & m_2^3 & m_3^3 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \oplus \begin{pmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

бу erда c_i ва s_i–кирувчи ва чиқувчи қийматларнинг i–бити ва $s=(s_0,s_1,s_2,s_3)$, $c=(c_0,c_1,c_2,c_3)$, $b=(b_0,b_1,b_2,b_3)$, $m^0=(m_0^0,m_1^0,m_2^0,m_3^0)$, $m^1=(m_0^1,m_1^1,m_2^1,m_3^1)$, $m^2=(m_0^2,m_1^2,m_2^2,m_3^2)$, $m^3=(m_0^3,m_1^3,m_2^3,m_3^3)$, $c=a^{-1}$. Агарда m^0, m^1, m^2, m^3, b–константа ва a ўзгарувчи нолдан 15 гача ўзгарса, у ҳолда ўлчами 4x4 бўлган S–блок генерация қилинади.

Ниберг конструкцияси асосида

– ўлчами 8x8 бўлган S–блоклар генерация усули ва дастурий таъминоти яратилди, S–блоклар учун $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, SAC=8, BIC=8 шартлар бажарилади, S–блоклар сони 32640 га тенг;

– саккизта ўзгарувчига эга буль функциялари генерация қилиш усули яратилди, бу буль функциялари учун $NL(f)=112$, $\deg(f)=7$, $Dd_j(f)\le 8$, $1\le j\le 8$ шартлар бажарилади, буль функциялар сони 256 га тенг ва генерация қилинган бул функциялари асосида S–блоклар яратиш мумкин, S–блоклар учун $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, SAC=8, BIC=8 шартлар бажарилади;

– ўлчами 4x4 бўлган S–блоклар ишлаб чиқиш усули ва дастурий таъминоти яратилди, бу S–блоклар учун $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC=2, BIC=4 шартлар бажарилади, S–блоклар сони 221760 га тенг;

– тўртта ўзгарувчига эга буль функциялари генерация қилиш усули яратилди, бу буль функциялари учун $NL(f)=4$, $\deg(f)=3$, $Dd_j(f)\le 4$, $1\le j\le 4$ шартлар бажарилади, буль функциялар сони 28 га тенг ва генерация қилинган бул функциялари асосида 236544 та S–блоклар яратилган, S–блоклар учун $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC=2, BIC=4 бажарилади.

Ниберг конструкцияси учун қуйидаги иккита тасдиқ ўринли:

Тасдиқ 1. *GenerSBox(m,b)* кўринишда Ниберг конструкцияси асосида ўлчами 8x8 бўлган 32640 та бардошли S–блок ва 256 та буль функциялар генерация қилинади.

Тасдиқ 2. *GenerSBox(m^0,m^1,m^2,m^3,b)* кўринишда Ниберг конструкция–си асосида ўлчами 4x4 бўлган 221760 та бардошли S–блок ва 28 та буль функциялар генерация қилинади.

S–блокларни бардошлилигини ҳисоблашда умумий мураккаблик кўрсаткичидан ҳам фойдаланилади. Умумий мураккаблик кўрсаткичи n=8 да қуйидагича аниқланган:

$$S^8_{index}=\frac{\frac{\deg(F)}{7}+\frac{NL(F)}{118}+\frac{258-\max XOR(a,b)}{256}+\frac{64-SAC}{64}+\frac{64-BIC}{64}}{5}$$

n=4 да умумий мураккаблик кўрсаткичи қуйидагича аниқланган:

$$S^4_{index}=\frac{\frac{\deg(F)}{3}+\frac{NL(F)}{4}+\frac{18-\max XOR(a,b)}{16}+\frac{16-SAC}{16}+\frac{16-BIC}{16}}{5}$$

Теорема 1. S–блок умумий мураккаблик кўрсаткичлари $0<S^8_{index}<1$, $0<S^4_{index}<1$ ва идеал S–блок учун $S^8_{index}=1$, $S^4_{index}=1$ бажарилади.

ГОСТ 28147–89 ва AES шифрлаш алгоритмлари учун қуйидаги тасдиқлар ўринли.

Тасдиқ 3. ГОСТ 28147–89 шифрлаш алгоритми биринчи ва тўртинчи S–блоки S^4_{index}=0,8, нолинчи S–блоки S^4_{index}=0,8083, иккинчи S–блоки S^4_{index}=0,775, учинчи ва еттинчи S–блоки S^4_{index}=0,6833, бешинчи S–блоки S^4_{index}=0,75, олтинчи S–блоки S^4_{index}=0,7083 га тенг.

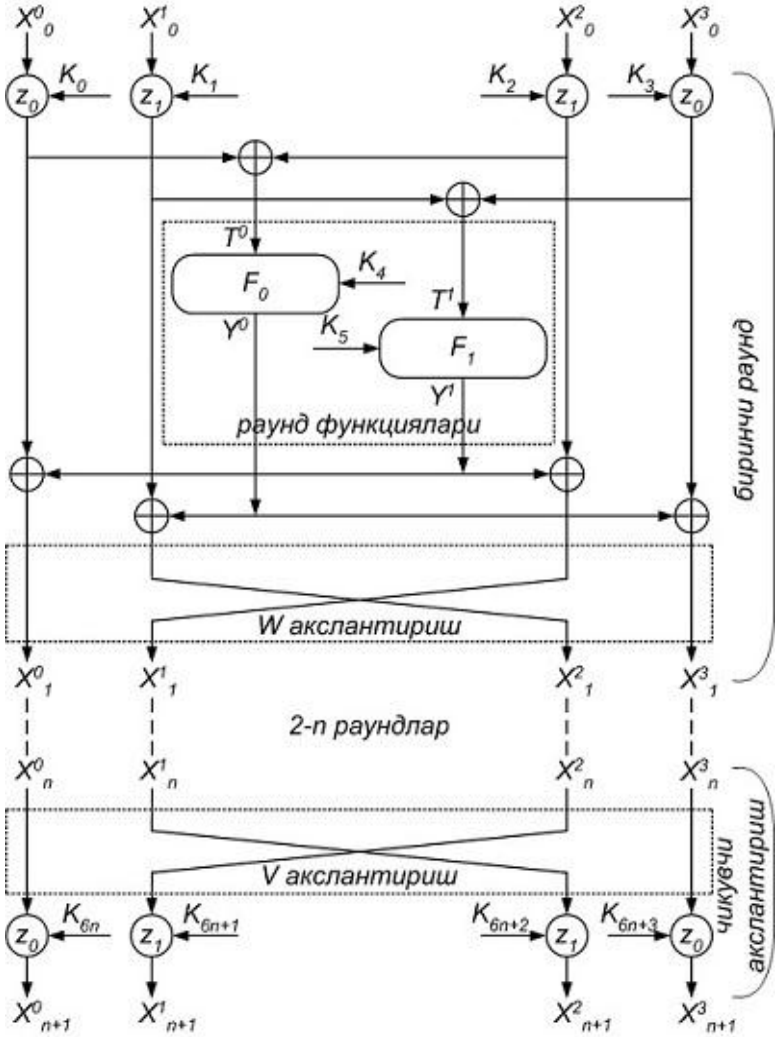
Тасдиқ 4. AES шифрлаш алгоритми S–блоки S^8_{index}=0,9382 га тенг.

Диссертациянинг **«IDEA шифрлаш алгоритми структураси ва Лай–Месси схемаси асосида ишлаб чиқилган IDEAX–Y, RFWKIDEAX–Y кўринишдаги Лай–Месси тармоқлари»** деб номланган иккинчи бобида IDEA шифрлаш алгоритми структураси ва Лай–Месси схемаси асосида ишлаб чиқилган IDEAX–Y, RFWKIDEAX–Y кўринишдаги Лай–Месси тармоқлари келтирилган, бу ерда X–қисм блоклар сони, Y–раунд функциялар сони. Тармоқларнинг асосий афзалликлари шундан иборатки, шифрлашда ва

дешифрлашда битта алгоритмдан фойдаланилади, тармоқ раунд функцияси сифатида исталган акслантиришларни олиш мумкин.

IDEA4–2 тармоғи 3–расмда келтирилган бўлиб, X_0, X_1, X_2, X_3 қисм блоклар, $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i=\overline{1...n+1}$ раунд калитлари, F_0, F_1 раунд функцияларга кирувчи ва раунд функциялардан чиқувчи қисм блоклар узунлиги 32 (16) битга тенг. $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$ раунд калитлари узунлиги эса 32 (16) битга тенг бўлиши шарт эмас.

Тармоқдаги z_0, z_1 амаллари сифатида $\otimes$ (mul), $\boxplus$ (add) ва $\oplus$ (xor) амалларини олинган. Бу ерда $\otimes$–32 (16) битли блокларни $2^{32}+1$ ($2^{16}+1$) модул бўйича кўпайтириш амали, $\boxplus$–32 (16) битли блокларни 2^{32} (2^{16}) модул бўйича қўшиш амали ва $\oplus$–32 (16) битли блокларни XOR бўйича қўшиш амали.



3–расм. IDEA4–2 тармоғи схемаси

n–раундли IDEA4–2 тармоғида ҳар бир раундда олтита ва чиқувчи акслантиришда тўртта раунд калити қўлланилган, яъни жами раунд калитлари сони 6*n*+4 га тенг. Шифрлашда 3–расмдаги K_i ўрнига K_i^c шифрлаш раунд калитлари, дешифрлашда эса K_i^d дешифрлаш раунд калитлари қўлланилади.

IDEA4–2 тармоғи биринчи раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (1) бўйича, чиқувчи акслантириш дешифрлаш раунд калитлари шифрлаш раунд калитларига (2) бўйича ва иккинчи, учинчи, *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (3) бўйича боғланган:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d) = ((K_{6n}^c)^{z_0}, (K_{6n+1}^c)^{z_1}, (K_{6n+2}^c)^{z_1}, (K_{6n+3}^c)^{z_0}, K_{6(n-1)+4}^c, K_{6(n-1)+5}^c) \quad (1)$$

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_1}, (K_2^c)^{z_1}, (K_3^c)^{z_0}) \quad (2)$$

$$(K_{6(i-1)}^d, K_{6(i-1)+1}^d, K_{6(i-1)+2}^d, K_{6(i-1)+3}^d, K_{6(i-1)+4}^d, K_{6(i-1)+5}^d) = ((K_{6(n-i+1)}^c)^{z_0}, (K_{6(n-i+1)+2}^c)^{z_1}, (K_{6(n-i+1)+1}^c)^{z_1}, (K_{6(n-i+1)+3}^c)^{z_0}, K_{6(n-i)+4}^c, K_{6(n-i)+5}^c), i = \overline{2...n}. \quad (3)$$

Агарда z_0, z_1 амаллар сифатида mul қўлланилса, $K = K^{-1}$, add қўлланилса, $K = -K$ ва xor қўлланилса, $K = K$, бу ерда $K^{-1} - K$ сонининг мультипликатив инверсияси, $-K - K$ сонининг аддитив инверсияси. 32 битли сонлар учун $K \otimes K^{-1} = 1 \bmod(2^{32}+1)$, 16 битли сонлар учун $K \otimes K^{-1} = 1 \bmod(2^{16}+1)$ ва $-K \boxplus K = 0$, $K \oplus K = 0$.

IDEA4–2 тармоғи учун қуйидаги теорема ўринли:

Теорема 2. IDEA4–2 тармоғи дешифрлаш раунд калитлари (1)–(3) формулалар орқали ҳисобланганда шифрлаш ва дешифрлашда ягона алгоритмга асосланган.

IDEA4–2 тармоғи асосида раунд функцияси иккита кирувчи ва чиқувчи қисм блокга эга, раунд функциясида битта раунд калити қўлланилган IDEA4–1 тармоғи, IDEA4–2 ва IDEA4–1 тармоқларини раунд функциялари калитсиз қўлланилган кўриниши бўлган RFWKIDEA4–2, RFWKIDEA4–1 тармоқлари ишлаб чиқилган.

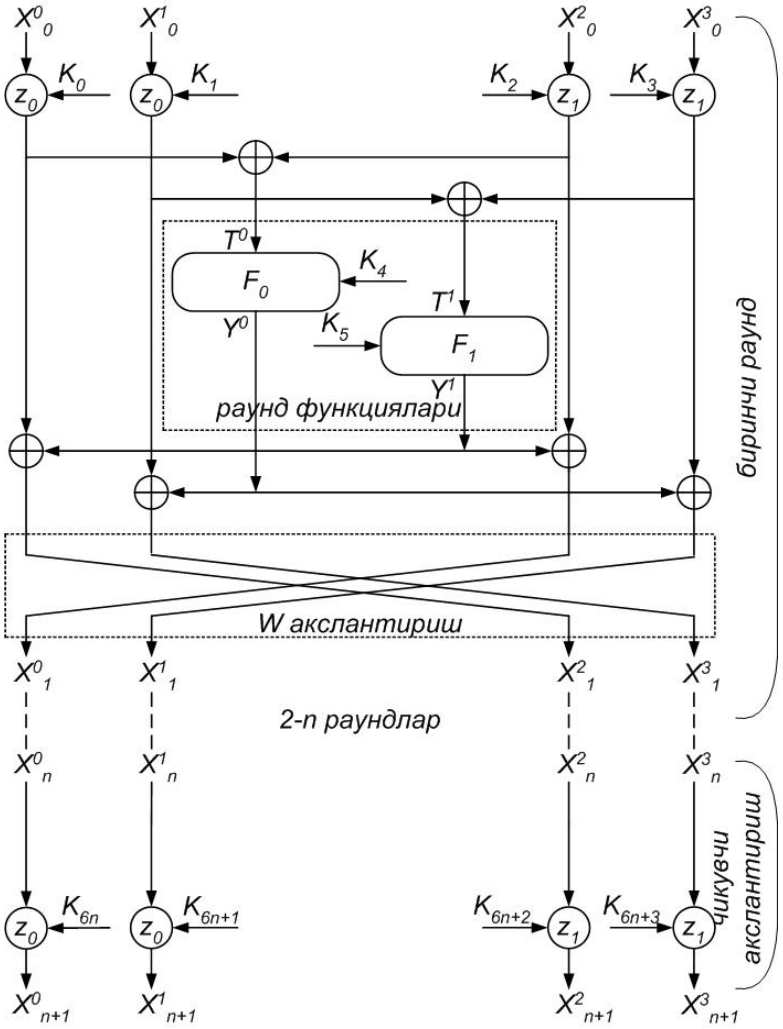
Худди шунингдек, саккизта, ўн олтита, ўттиз иккита ва 2m та қисм блокдан ташкил топган тармоқлар ишлаб чиқилган. Умумий ҳолатда тармоқларни IDEAX–Y, RFWKIDEAX–Y кўринишга келтириш мумкин, бу ерда X–қисм блоклар сони, Y–раунд функциялар сони. IDEAX–Y кўринишдаги тармоқда раунд калитлари сони (X+Y)n+X га, RFWKIDEAX–Y кўринишдаги тармоқда эса Xn+X га тенг. Масалан, IDEA8–4 тармоғи саккизта қисм блок ва тўртта раунд функциядан ташкил топган бўлиб, ҳар бир раунд функциясига битта қисм блок киради ва чиқади, RFWKIDEA32–2 тармоғи ўттиз иккита қисм блок ва иккита раунд функциядан ташкил топган бўлиб, ҳар бир раунд функциясига қирувчи ва чиқувчи қисм блоклар сони саккизга тенг. Раунд функцияларга кирувчи ва чиқувчи қисм блоклар сони R=(X/Y)/2 бўйича ҳисобланади.

IDEAX–Y, RFWKIDEAX–Y (X>4) кўринишдаги тармоқларда амаллар сони X/2 га тенг бўлиб, амаллари сифатида ⊗–32 (16, 8) битли блокларни $2^{32}+1$ ($2^{16}+1$, 2^8+1) модул бўйича кўпайтириш, ⊞–32 (16, 8) битли блокларни 2^{32} (2^{16}, 2^8) модул бўйича қўшиш ва ⊕–32 (16, 8) битли блокларни XOR бўйича қўшиш амаллари олинган.

Диссертациянинг **«PES шифрлаш алгоритми структураси ва Лай–Месси схемаси асосида ишлаб чиқилган PESX–Y, RFWKPESX–Y кўринишдаги Лай–Месси тармоқлари»** деб номланган учинчи бобида PES

шифрлаш алгоритми структураси ва Лай–Месси схемаси асосида ишлаб чиқилган PESX–Y, RFWKPESX–Y кўринишдаги Лай–Месси тармоқлари келтирилган. Тармоқларнинг асосий афзалликлари шундан иборатки, шифрлашда ва дешифрлашда битта алгоритмдан фойдаланилади, тармоқ раунд функцияси сифатида исталган акслантиришларни олиш мумкин.

PES4–2 тармоғи 4–расмда келтирилган бўлиб, X^0, X^1, X^2, X^4 қисм блоклар, $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i=\overline{1...n+1}$ раунд калитлари, F_0, F_1 раунд функцияларга кирувчи ва раунд функциядан чиқувчи қисм блоклар узунлиги 32 (16) битга тенг. $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$ раунд калитлари узунлиги эса 32 (16) битга тенг бўлиши шарт эмас.



4–расм. PES4–2 тармоғи схемаси

n–раундли PES4–2 тармоғида ҳар бир раундда олтита ва чиқувчи акслантиришда тўртта раунд калити иштирок этади, яъни жами раунд калитлари сони 6*n*+4 га тенг. PES4–2 тармоғи чиқувчи акслантириш дешифрлаш раунд калитлари шифрлаш раунд калитларига (4) бўйича, биринчи, иккинчи ва *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (5) бўйича боғланган:

$$(K^d_{6n}, K^d_{6n+1}, K^d_{6n+2}, K^d_{6n+3}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_1}, (K^c_3)^{z_1}) \qquad (4)$$

$$(K^d_{6(i-1)}, K^d_{6(i-1)+1}, K^d_{6(i-1)+2}, K^d_{6(i-1)+3}, K^d_{6(i-1)+4}, K^d_{6(i-1)+5}) = ((K^c_{6(n-i+1)})^{z_0}, (K^c_{6(n-i+1)+1})^{z_0}, (K^c_{6(n-i+1)+2})^{z_1}, (K^c_{6(n-i+1)+3})^{z_1}, K^c_{6(n-i)+4}, K^c_{6(n-i)+5}), i = \overline{1...n}. \quad (5)$$

PES4–2 тармоғи учун қуйидаги теорема ўринли:

Теорема 3. PES4–2 тармоғи дешифрлаш раунд калитлари (4), (5) формулалар орқали ҳисобланганда шифрлаш ва дешифрлашда ягона алгоритмга асосланган.

Худди шунингдек, тўртта, саккизта, ўн олтита, ўттиз иккита ва 2m та қисм блокдан ташкил топган тармоқлар ишлаб чиқилган. Умумий ҳолатда тармоқларни PESX–Y, RFWKPESX–Y кўринишга келтириш мумкин, IDEAX–Y кўринишдаги тармоқда раунд калитлари сони (X+Y)n+X га, RFWKIDEAX–Y кўринишдаги тармоқда эса Xn+X га тенг. Масалан, PES16–4 тармоғи ўн олтита қисм блок ва тўртта раунд функциядан ташкил топган бўлиб, ҳар бир раунд функциясига иккита кирувчи ва чиқувчи қисм блокга эга.

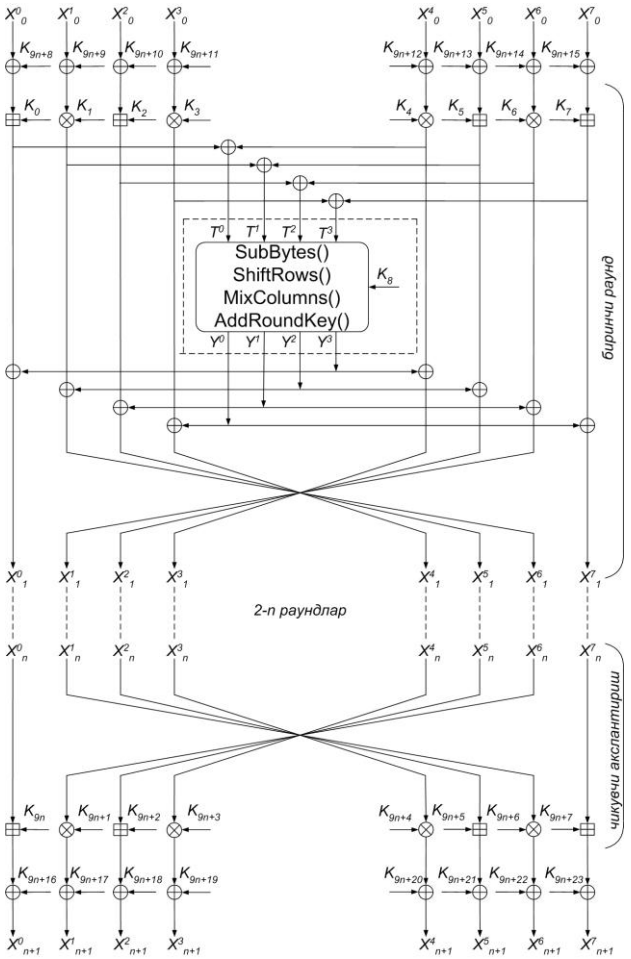
PESX–Y, RFWKPESX–Y кўринишдаги тармоқларда амаллар сони иккита бўлиб, амаллари сифатида ⊗–32 (16, 8) битли блокларни $2^{32}+1$ ($2^{16}+1$, 2^8+1) модул бўйича кўпайтириш, ⊞–32 (16, 8) битли блокларни 2^{32} (2^{16}, 2^8) модул бўйича қўшиш ва ⊕–32 (16, 8) битли блокларни XOR бўйича қўшиш амаллари олинган.

Диссертациянинг **«AES шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида ишлаб чиқилган шифрлаш алгоритмлари»** деб номланган тўртинчи бобида AES шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш ҳисобига ишлаб чиқилган шифрлаш алгоритмлари келтирилган, тезлиги ва бардошлиги баҳоланган.

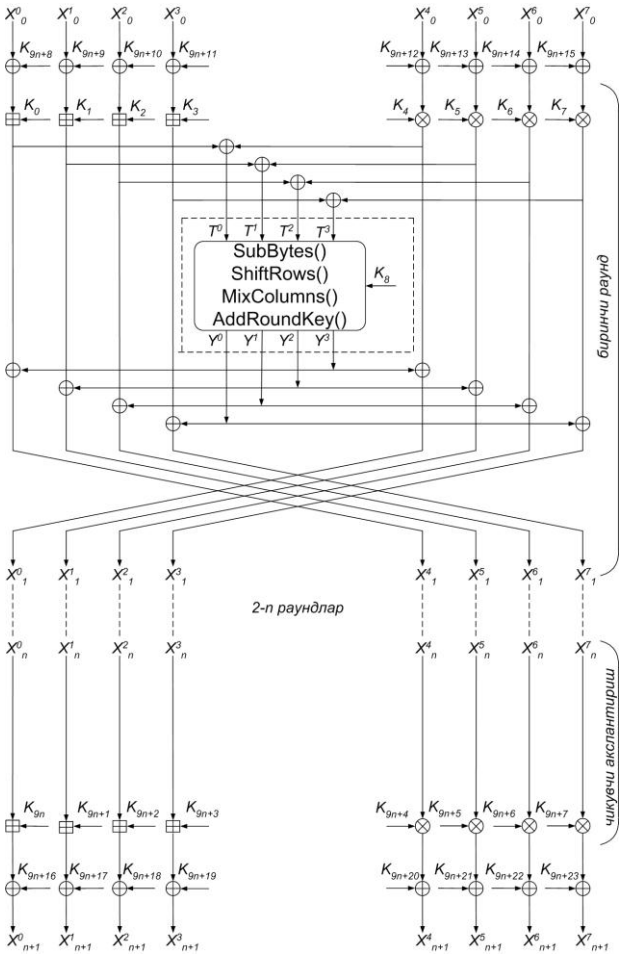
AES–IDEA8–1 ва AES–PES8–1 шифрлаш алгоритмлари схемаси 5 ва 6–расмларда келтирилган бўлиб X^0, X^1, ..., X^7 қисм блоклар, $K_{9(i-1)}$, $K_{9(i-1)+1}$, ..., $K_{9(i-1)+7}$, $i = \overline{1...n+1}$, K_{9n+8}, K_{9n+9}, ..., K_{9n+23} раунд калитлари узунлиги 32 битга тенг. $K_{9(i-1)+8}$, $i = \overline{1...n}$ раунд калити узунлиги эса 128 битга тенг ва бу калит AddRoundKey() акслантириши калит массиви сифатида олинади. Шифрлаш алгоритмларида AES шифрлаш алгоритмининг SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() акслантиришлари қўлланилган.

Шифрлаш алгоритмлари раунд функциясида 32 битли T^0, T^1, ..., T^3 қисм блоклар 8 битли қисм блокларга ажратилади, яъни $t_i = sb_{i \bmod 4}(T^{idiv4})$, $i = \overline{0...15}$. Бу ерда div–бўлинманинг бутун қисми, mod–бўлинманинг қолдиқ қисми, $sb_0(X) = x_0x_1...x_7$, $sb_1(X) = x_8x_9...x_{15}$, $sb_2(X) = x_{16}x_{17}...x_{23}$, $sb_3(X) = x_{24}x_{25}...x_{31}$ ва $X = x_0x_1...x_{31}$. 8 битли t_0, t_1, ... t_{15} қисм блоклар State массивига ёзилади. AddRoundKey() акслантиришида 128 битли $K_{9(i-1)+8}$ раунд калити 32 битли $K^0_{9(i-1)+8}$, $K^1_{9(i-1)+8}$, $K^2_{9(i-1)+8}$, $K^3_{9(i-1)+8}$ раунд калитларига бўлинади. 32 битли $K^0_{9(i-1)+8}$, $K^1_{9(i-1)+8}$, $K^2_{9(i-1)+8}$, $K^3_{9(i-1)+8}$ калитлар 8 битли k_0, k_1, ..., k_{15} калитларга ажратилади, яъни $k_i = sb_{i \bmod 4}(K^{idiv4}_{9(i-1)+8})$. Сўнгра SubBytes(),

ShiftRows(), MixColumns(), AddRoundKey() акслантиришлари бажарилади. AddRoundKey() акслантиришидан сўнг 8 битли p'_0, p'_1, ..., p'_{15} қисм блоклар ҳосил бўлади. Ҳосил бўлган 8 битли p'_0, p'_1, ..., p'_{15} қисм блоклар 32 битли Y^0, Y^1, …, Y^3 қисм блокларга қуйидагича ёзилади: $Y^j = p'_{4j} \| p'_{4j+1} \| p'_{4j+2} \| p'_{4j+3}$, $j = \overline{0...3}$.



5–расм. AES–IDEA8–1 шифрлаш алгоритми схемаси



6–расм. AES–PES8–1 шифрлаш алгоритми схемаси

n–раундли AES–IDEA8–1 ва AES–PES8–1 шифрлаш алгоритмларида ҳар бир раундда саккизта 32 битли, битта 128 битли ва чиқувчи акслантиришда саккизта 32 битли раунд калитлари қўлланилади. Бундан ташқари биринчи раундгача ва чиқувчи акслантиришдан сўнг саккизта 32 битли раунд калитлари иштирок этган. 128 битли калит тўртта 32 битли калит сифатида қабул қилинса, барча 32 битли раунд калитлари сони 12*n*+24 га тенг.

Шифрлаш алгоритмлари шифрлаш раунд калитларини ҳосил қилишда AES шифрлаш алгоритми каби Rcon массивидан фойдаланилади. Rcon=[0x00000001, 0x00000002, 0x00000004, 0x00000008, 0x00000010, 0x00000020, 0x00000040, 0x00000080, 0x00000100, 0x00000200, 0x00000400, 0x00000800, 0x00001000, 0x00002000, 0x00004000, 0x00008000, 0x00010000, 0x00020000, 0x00040000, 0x00080000, 0x00100000, 0x00200000, 0x00400000, 0x00800000, 0x01000000, 0x02000000, 0x04000000, 0x08000000, 0x10000000,

0x20000000, 0x40000000, 0x80000000], яъни ўттиз иккита 32 битли қийматдан ташкил топган.

Шифрлаш алгоритмларининг узунлиги l ($256 \le l \le 1024$) битга тенг K калити 32 битли $K_0^{c'}$, $K_1^{c'}$, ..., $K_{Lenght-1}^{c'}$, $Lenght = l/32$ калитларга ажратилади, бу ерда $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^{c'} = \{k_0, k_1, ..., k_{31}\}$, $K_1^{c'} = \{k_{32}, k_{33}, ..., k_{63}\}$, ..., $K_{Lenght-1}^{c'} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ ва $K = K_0^{c'} \| K_1^{c'} \| ... \| K_{Lenght-1}^{c'}$. Сўнгра $K_L = K_0^{c'} \oplus K_1^{c'} \oplus ... \oplus K_{Lenght-1}^{c'}$ ҳисобланади. Агарда $K_L = 0$ бўлса, у ҳолда K_L сифатида 0xC5C31537 қиймат олинади, яъни $K_L = 0$xC5C31537. $K_i^{c'}$, $i = \overline{Lenght...12n+23}$ раунд калитлари эса $i \bmod 3 = 1$ шарт бажарилганда $K_i^{c'} = SubBytes32(K_{i-Lenght+1}^{c'}) \oplus SubBytes32(RotWord32(K_{i-Lenght}^{c'})) \oplus Rcon[i \bmod 32] \oplus K_L$ каби, акс ҳолда $K_i^{c'} = SubBytes32(K_{i-Lenght}^{c'}) \oplus SubBytes32(K_{i-Lenght+1}^{c'}) \oplus K_L$ каби ҳисобланади. Ҳар бир раунд калити генерация қилингандан сўнг K_L қиймат чапга бир бит циклик сурилади. Бу ерда *Rotword32()*–32 битли блокни чапга бир бит циклик суриш акслантириши, *SubBytes32()*–32 битли блокни S–блокда ўрнига қўйиш акслантириши, яъни $SubBytes32(X) = S(sb_0(X)) \| S(sb_1(X)) \| S(sb_2(X)) \| S(sb_3(X))$.

AES–IDEA8–1 шифрлаш алгоритми биринчи раунд дешифрлаш калитлари шифрлаш раунд калитларига (6) бўйича, чиқувчи акслантириш дешифрлаш раунд калитлари шифрлаш раунд калитларига (7) бўйича, иккинчи, учинчи, *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (8) бўйича боғланган:

$$(K_0^{d'}, K_1^{d'}, K_2^{d'}, K_3^{d'}, K_4^{d'}, K_5^{d'}, K_6^{d'}, K_7^{d'}, K_8^{d'}, K_9^{d'}, K_{10}^{d'}, K_{11}^{d'}) = (-K_{12n}^{c'}, (K_{12n+1}^{c'})^{-1}, -K_{12n+2}^{c'}, (K_{12n+3}^{c'})^{-1}, (K_{12n+4}^{c'})^{-1}, -K_{12n+5}^{c'}, (K_{12n+6}^{c'})^{-1}, -K_{12n+7}^{c'}, K_{12(n-1)+8}^{c'}, K_{12(n-1)+9}^{c'}, K_{12(n-1)+10}^{c'}, K_{12(n-1)+11}^{c'}). \quad (6)$$

$$(K_{12n}^{d'}, K_{12n+1}^{d'}, K_{12n+2}^{d'}, K_{12n+3}^{d'}, K_{12n+4}^{d'}, K_{12n+5}^{d'}, K_{12n+6}^{d'}, K_{12n+7}^{d'}) = (-K_0^{c'}, (K_1^{c'})^{-1}, -K_2^{c'}, (K_3^{c'})^{-1}, (K_4^{c'})^{-1}, -K_5^{c'}, (K_6^{c'})^{-1}, -K_7^{c'}). \quad (7)$$

$$(K_{12(i-1)}^{d'}, K_{12(i-1)+1}^{d'}, K_{12(i-1)+2}^{d'}, K_{12(i-1)+3}^{d'}, K_{12(i-1)+4}^{d'}, K_{12(i-1)+5}^{d'}, K_{12(i-1)+6}^{d'}, K_{12(i-1)+7}^{d'}, K_{12(i-1)+8}^{d'}, K_{12(i-1)+9}^{d'}, K_{12(i-1)+10}^{d'}, K_{12(i-1)+11}^{d'}) = (-K_{12(n-i+1)}^{c'}, (K_{6(n-i+1)+6}^{c'})^{-1}, -K_{12(n-i+1)+5}^{c'}, (K_{12(n-i+1)+4}^{c'})^{-1}, (K_{12(n-i+1)+3}^{c'})^{-1}, -K_{6(n-i+1)+2}^{c'}, (K_{12(n-i+1)+1}^{c'})^{-1}, -K_{12(n-i+1)+7}^{c'}, K_{12(n-i)+8}^{c'}, K_{12(n-i)+9}^{c'}, K_{12(n-i)+10}^{c'}, K_{12(n-i)+11}^{c'}), i = \overline{2...n}. \quad (8)$$

AES–PES8–1 шифрлаш алгоритми биринчи, иккинчи *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (9) бўйича, чиқувчи акслантириш дешифрлаш раунд калитлари шифрлаш раунд калитларига (10) бўйича боғланган:

$$(K_{12(i-1)}^{d'}, K_{12(i-1)+1}^{d'}, K_{12(i-1)+2}^{d'}, K_{12(i-1)+3}^{d'}, K_{12(i-1)+4}^{d'}, K_{12(i-1)+5}^{d'}, K_{12(i-1)+6}^{d'}, K_{12(i-1)+7}^{d'}, K_{12(i-1)+8}^{d'}, K_{12(i-1)+9}^{d'}, K_{12(i-1)+10}^{d'}, K_{12(i-1)+11}^{d'}) = (-K_{12(n-i+1)}^{c'}, -K_{12(n-i+1)+1}^{c'}, -K_{12(n-i+1)+2}^{c'}, -K_{12(n-i+1)+3}^{c'}, (K_{12(n-i+1)+4}^{c'})^{-1}, (K_{12(n-i+1)+5}^{c'})^{-1}, (K_{12(n-i+1)+7}^{c'})^{-1}, (K_{12(n-i+1)+7}^{c'})^{-1}, K_{12(n-i)+8}^{c'}, K_{12(n-i)+9}^{c'}, K_{12(n-i)+10}^{c'}, K_{12(n-i)+11}^{c'}), i = \overline{1...n}. \quad (9)$$

$$(K_{12n}^{d'}, K_{12n+1}^{d'}, K_{12n+2}^{d'}, K_{12n+3}^{d'}, K_{12n+4}^{d'}, K_{12n+5}^{d'}, K_{12n+6}^{d'}, K_{12n+7}^{d'}) = (-K_0^{c'}, -K_1^{c'}, -K_2^{c'}, -K_3^{c'}, (K_4^{c'})^{-1}, (K_5^{c'})^{-1}, (K_6^{c'})^{-1}, (K_7^{c'})^{-1}). \quad (10)$$

Биринчи раундгача ва чиқувчи акслантиришдан сўнг қўлланилган дешифрлаш раунд калитлари шифрлаш раунд калитларига қуйидагича боғланган: $K_{12n+8+j}^{d'} = K_{12n+16+j}^{c'}$, $K_{12n+16+j}^{d'} = K_{12n+8+j}^{c'}$, $j = \overline{0...7}$.

K_i^c шифрлаш раунд калити $K_i^{c'}$ калитга қуйидагича боғланган: $K_{9i+j}^c = K_{12i+j}^{c'}$, $j = \overline{0...7}$, $K_{9i+8}^c = K_{12i+8}^{c'} \| K_{12i+9}^{c'} \| K_{12i+10}^{c'} \| K_{12i+11}^{c'}$, $K_{9n+j}^c = K_{12n+j}^{c'}$, $j = \overline{0...7}$, $K_{9n+8+j}^c = K_{12n+8+j}^{c'}$, $j = \overline{0...15}$. Худди шунингдек, K_i^d дешифрлаш раунд калити $K_i^{d'}$ калитга қуйидагича боғланган: $K_{9i+j}^d = K_{12i+j}^{d'}$, $j = \overline{0...7}$, $K_{9i+8}^d = K_{12i+8}^{d'} \| K_{12i+9}^{d'} \| K_{12i+10}^{d'} \| K_{12i+11}^{d'}$, $K_{9n+j}^d = K_{12n+j}^{d'}$, $j = \overline{0...7}$, $K_{9n+8+j}^d = K_{12n+8+j}^{d'}$, $j = \overline{0...15}$.

IDEAX–Y, PESX–Y, RFWKIDEAX–Y, RFWKPESX–Y кўринишдаги тармоқлар раунд функциялари сифатида AES алгоритми акслантиришларини қўллаш ҳисобига AES–IDEAX–Y, AES–PESX–Y, AES–RFWKIDEAX–Y, AES–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилган. AES–IDEAX–Y, AES–PESX–Y кўринишдаги алгоритмларда SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() акслантириши қўлланилган бўлса, AES–RFWKIDEAX–Y, AES–RFWKPESX–Y кўринишдаги шифрлаш алгоритмларда SubBytes(), ShiftRows(), MixColumns() акслантириши қўлланилган. Барча шифрлаш алгоритмлари калит узунлиги 256 битдан 1024 битгача 128 бит қадам билан ўзгаради. AES–IDEA8–1, AES–PES8–1, AES–RFWKIDEA8–1, AES–RFWKPES8–1, AES–IDEA16–1, AES–PES16–1, AES–RFWKIDEA16–1, AES–RFWKPES16–1, AES–IDEA32–1, AES–PES32–1, AES–RFWKIDEA32–1, AES–RFWKPES32–1 шифрлаш алгоритмлари блок узунлиги 256 битга, AES–IDEA16–2, AES–PES16–2, AES–RFWKIDEA16–2, AES–RFWKPES16–2 шифрлаш алгоритмлари блок узунлиги 512 битга, AES–IDEA32–4, AES–PES32–4, AES–RFWKIDEA32–4, AES–RFWKPES32–4 шифрлаш алгоритмлари блок узунлиги 1024 битга тенг. AES–IDEA16–1, AES–PES16–1, AES–RFWKIDEA16–1, AES–RFWKPES16–1 шифрлаш алгоритмлари қисм блоклари узунлиги 16 битга, AES–IDEA32–1, AES–PES32–1, AES–RFWKIDEA32–1, AES–RFWKPES32–1 шифрлаш алгоритмлари қисм блоклари узунлиги 8 битга ва қолган бошқа алгоритмлар қисм блоклари узунлиги 32 битга тенг. Шифрлаш алгоритмларнинг тезликлари 3–жадвалда келтирилган.

Шифрлаш алгоритмларининг S–блоклари параметрлари AES шифрлаш алгоритми параметрларига тенг, яъни $\deg(S) = 7$, $NL(S) = 112$, $\lambda_F = 0.125$, $\delta_F = 1/64$, SAC=8, BIC=8. Шифрлаш алгоритмлари учун қуйидаги тасдиқ ўринли:

Тасдиқ 5. AES–IDEAX–Y, AES–PESX–Y, AES–RFWKIDEAX–Y, AES–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари S–блоклари умумий мураккаблик кўрсаткичи S_{index}^8=0,9382 га тенг, яъни AES шифрлаш алгоритми умумий мураккаблик кўрсаткичига тенг.

AES–IDEA8–1, AES–PES8–1, AES–RFWKIDEA8–1, AES–RFWKPES8–1, AES–IDEA16–1, AES–PES16–1, AES–RFWKIDEA16–1, AES–RFWKPES16–1, AES–IDEA32–1, AES–PES32–1, AES–RFWKIDEA32–1, AES–RFWKPES32–1 шифрлаш алгоритмларининг исталган блокидаги ўзгариши кўпи билан икки раунддан сўнг, қолган барча шифрлаш алгоритмларида эса кўпи билан уч раунддан сўнг таъсир этади. Шунингдек,

барча шифрлаш алгоритмларда калитнинг битта бити ўзгариши биринчи раунддан сўнг барча блокларга таъсир этади.

3–жадвал

Шифрлаш алгоритмлари тезликлари (Мбайт/с)

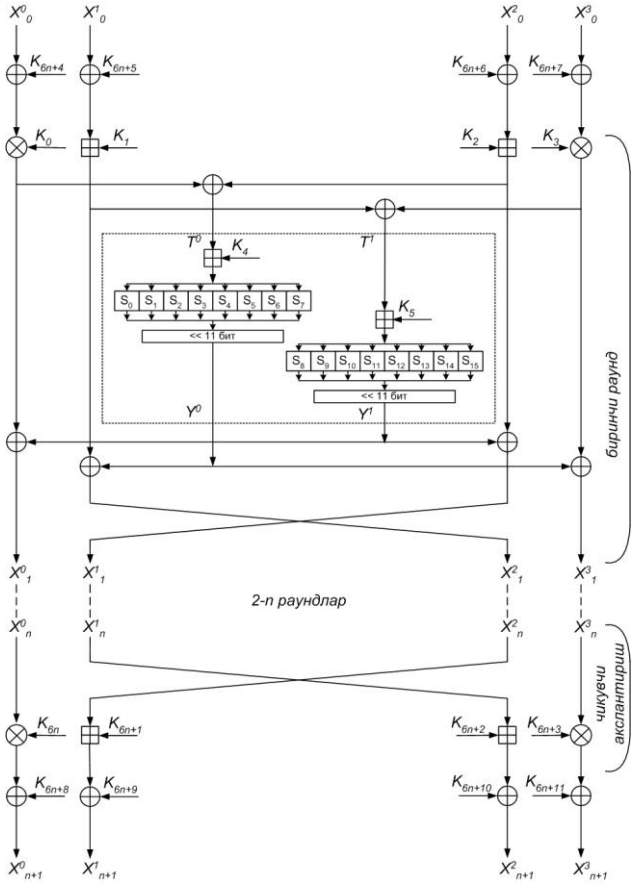
Шифрлаш алгоритми	10 раундли	12 раундли	14 раундли
AES	≈12.812	≈10.682	≈9.224
AES–IDEA8–1, AES–PES8–1	≈14.914	≈12.444	≈10.862
AES–RFWKIDEA8–1	≈16.862	≈14.244	≈12.330
AES–RFWKPES8–1	≈16.862	≈14.244	≈12.330
AES–IDEA16–1, AES–PES16–1	≈15.444	≈12.952	≈11.242
AES–RFWKIDEA16–1	≈17.808	≈14.902	≈12.944
AES–RFWKPES16–1	≈17.808	≈14.902	≈12.944
AES–IDEA32–1, AES–PES32–1	≈15.534	≈13.080	≈11.248
AES–RFWKIDEA32–1	≈17.094	≈14.566	≈12.444
AES–RFWKPES32–1	≈17.094	≈14.566	≈12.444
AES–IDEA16–2, AES–PES16–2	≈15.082	≈12.570	≈10.770
AES–RFWKIDEA16–2	≈17.294	≈14.082	≈12.330
AES–RFWKPES16–2	≈17.294	≈14.082	≈12.330
AES–IDEA32–4, AES–PES32–4	≈15.082	≈12.820	≈10.774
AES–RFWKIDEA32–4	≈16.876	≈14.184	≈12.210
AES–RFWKPES32–4	≈16.876	≈14.184	≈12.210

Шифрлаш алгоритмларига чизиқли криптотаҳлил усули қўлланилди. Криптотаҳлил усули қўллаш жараёнида кўпайтириш ўрнига қўшиш амали қўлланилди ва биринчи раундгача қўлланиган амаллар ҳисобга олинмади. Ҳисоблаш натижалари шуни кўрсатадики, барча шифрлаш алгоритмлари бардошлилиги тенг. 4 раундли шифрлаш алгоритмларига чизиқли криптотаҳлил усулини қўллаш учун $2^{30.6}$ та очиқ матн–шифрмат жуфтлиги, 8 раунд учун $2^{61.1}$ та очиқ матн–шифрмат жуфтлиги ва 12 раунд учун $2^{91.1}$ та очиқ матн–шифрмат жуфтлиги керак бўлади. Битта раунд учун эса 202 та очиқ матн–шифрмат жуфтлиги керак бўлади ва чизиқли аппроксимация тенгламалари сони 40 га тенг. Кўриниб турибдики, кўпайтириш амали ўрнига қўшиш амали фойдаланилгани ва биринчи раундгача қўлланиган амаллар ҳисобга олинмаган тақдирда ҳам шифрлаш бардошлиги нисбатан юқори.

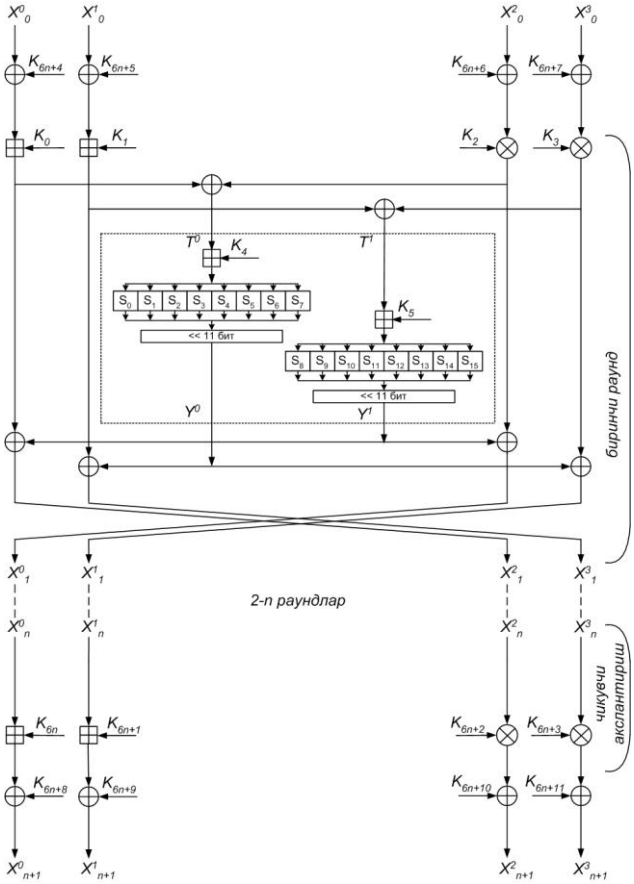
Диссертациянинг **«ГОСТ 28147–89 шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида ишлаб чиқилган шифрлаш алгоритмлари»** деб номланган бешинчи бобида ГОСТ 28147–89 шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш ҳисобига ишлаб чиқилган шифрлаш алгоритмлари келтирилган ва тезлиги, бардошлиги баҳоланган.

GOST28147–89–IDEA4–2 ва GOST28147–89–PES4–2 шифрлаш алгоритмларида схемаси 7 ва 8–расмларда келтирилган бўлиб, X^0, X^1, X^2, X^3 қисм блоклар, $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i=\overline{1...n+1}$, $K_{6(i-1)+4}$, $K_{6(i-1)+5}$,

$i=\overline{1...n}$, K_{6n+4}, K_{6n+5}, ..., K_{6n+11} раунд калитлари, раунд функцияга кирувчи ва чиқувчи қисм блоклар узунлиги 32 битга тенг.



7–расм. GOST28147–89–IDEA4–2 шифрлаш алгоритми



8–расм. GOST28147–89–PES4–2 шифрлаш алгоритми

Шифрлаш алгоритмлари раунд функциясида 32 битли T^0, T^1 қисм блокларга $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$ раунд калитлари қўшилади, яъни $S^0=T^0+K_{6(i-1)+4}$, $S^1=T^1+K_{6(i-1)+5}$. 32 битли S^0, S^1 қисм блоклар саккизта тўрт битли қисм блокларга бўлинади $S^0=s_0^0\|s_1^0\|s_2^0\|s_3^0\|s_4^0\|s_5^0\|s_6^0\|s_7^0$, $S^1=s_0^1\|s_1^1\|s_2^1\|s_3^1\|s_4^1\|s_5^1\|s_6^1\|s_7^1$. 4 битли s_i^0, s_i^1, $i=\overline{0...7}$ қисм блоклар S–блокларда акслантирилади, яъни $R^0=S_0(s_0^0)\|S_1(s_1^0)\|S_2(s_2^0)\|S_3(s_3^0)\|S_4(s_4^0)\|S_5(s_5^0)\|S_6(s_6^0)\|S_7(s_7^0)$, $R^1=S_8(s_0^1)\|S_9(s_1^1)\|S_{10}(s_2^1)\|S_{11}(s_3^1)\|S_{12}(s_4^1)\|S_{13}(s_5^1)\|S_{14}(s_6^1)\|S_{15}(s_7^1)$. Ҳосил бўлган 32 битли R^0, R^1 қисм блоклар чапга 11 бит циклик сурилади ва Y^0, Y^1 қисм блоклар ҳосил бўлади: $Y^0=R^0<<11$, $Y^1=R^1<<11$.

n–раундли GOST28147–89–IDEA4–2 ва GOST28147–89–PES4–2 шифрлаш алгоритмида биринчи раундгача ва чиқувчи акслантиришдан сўнг сўнг тўртта 32 битли раунд калитлари, ҳар бир раундда олтита 32 битли раунд калитлари ва чиқувчи акслантиришда тўртта 32 битли раунд калити иштирок этади, яъни жами раунд калитлари сони 6*n*+12 га тенг. Шифрлаш алгоритми раундлар сони 8, 12 ва 16 га тенг бўлганда 32 битли 60, 84 ва 108 раунд калитлари генерация қилинади.

Шифрлаш алгоритмининг узунлиги l ($256 \le l \le 1024$) битга тенг бўлган дастлабки K калити 32 битли K_0^c, K_1^c, ..., $K_{Lenght-1}^c$, $Lenght = l/32$ ажратилади, бу ерда $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, ..., k_{63}\}$, ..., $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ ва $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$. Сўнгра $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$ ҳисобланади. Агарда $K_L = 0$ бўлса, у ҳолда K_L сифатида 0xC5C31537 қиймат олинади. K_i^c, $i = \overline{Lenght...6n+11}$ раунд калитлари эса $K_i^c = SBox0(K_{i-Lenght}^c) \oplus SBox1(RotWord(K_{i-Lenght+1}^c)) \oplus K_L$ каби ҳисобланади ҳар бир раунд калити генерация қилингандан сўнг K_L қиймат бир бит чапга сурилади. Бу ерда *Rotword()*–32 битли блокни чапга бир бит суриш акслантириши ва *Sbox()*–32 битли блокни S–блокда ўрнига қўйиш акслантириши ва $SBox0(A) = S_0(a_0) \| S_1(a_1) \| S_2(a_2) \| S_3(a_3) \| S_4(a_4) \| S_5(a_5) \| S_6(a_6) \| S_7(a_7)$, $SBox1(A) = S_8(a_0) \| S_9(a_1) \| S_{10}(a_2) \| S_{11}(a_3) \| S_{12}(a_4) \| S_{13}(a_5) \| S_{14}(a_6) \| S_{15}(a_7)$, $A = a_0 \| a_1 \| a_2 \| a_3 \| a_4 \| a_5 \| a_6 \| a_7$, бу ерда a_i – тўрт битли қисм блоклар.

GOST28147–89–IDEA4–2 шифрлаш алгоритми биринчи раунд дешифрлаш калитлари шифрлаш раунд калитларига (11) бўйича, чиқувчи акслантириш дешифрлаш раунд калитлари эса шифрлаш раунд калитларига (12) бўйича, иккинчи, учинчи, *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (13) бўйича боғланган:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d) = ((K_{6n}^c)^{-1}, -K_{6n+1}^c, -K_{6n+2}^c, (K_{6n+3}^c)^{-1}, K_{6(n-1)+4}^c, K_{6(n-1)+5}^c) \quad (11)$$

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = ((K_0^c)^{-1}, -K_1^c, -K_2^c, (K_3^c)^{-1}) \quad (12)$$

$$\begin{aligned}(K_{6(i-1)}^d, K_{6(i-1)+1}^d, K_{6(i-1)+2}^d, K_{6(i-1)+3}^d, K_{6(i-1)+4}^d, K_{6(i-1)+5}^d) = ((K_{6(n-i+1)}^c)^{-1}, -K_{6(n-i+1)+2}^c, \\ -K_{6(n-i+1)+1}^c, (K_{6(n-i+1)+3}^c)^{-1}, K_{6(n-i)+4}^c, K_{6(n-i)+5}^c), i = \overline{2...n}.\end{aligned} \quad (13)$$

GOST28147–89–PES4–2 шифрлаш алгоритмлари чиқувчи акслантириш дешифрлаш раунд калитлари эса шифрлаш раунд калитларига (14) бўйича, биринчи, иккинчи, *n*–раунд дешифрлаш раунд калитлари шифрлаш раунд калитларига (15) бўйича боғланган:

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = (-K_0^c, -K_1^c, (K_2^c)^{-1}, (K_3^c)^{-1}) \quad (14)$$

$$\begin{aligned}(K_{6(i-1)}^d, K_{6(i-1)+1}^d, K_{6(i-1)+2}^d, K_{6(i-1)+3}^d, K_{6(i-1)+4}^d, K_{6(i-1)+5}^d) = (-K_{6(n-i+1)}^c, -K_{6(n-i+1)+1}^c, \\ (K_{6(n-i+1)+2}^c)^{-1}, (K_{6(n-i+1)+3}^c)^{-1}, K_{6(n-i)+4}^c, K_{6(n-i)+5}^c), i = \overline{1...n}.\end{aligned} \quad (15)$$

Биринчи раунддан олдин ва чиқувчи акслантиришдан сўнг қўлланилган дешифрлаш калитлари шифрлаш калитларига қуйидагича боғланган: $K_{6n+4+j}^d = K_{6n+8+j}^c$, $K_{6n+8+j}^d = K_{6n+4+j}^c$, $j = \overline{0...3}$.

IDEAX–Y, PESX–Y, RFWKIDEAX–Y, RFWKPESX–Y кўринишдаги тармоқлар раунд функциялари сифатида ГОСТ 28147–89 шифрлаш алгоритми акслантиришларидан фойдаланган ҳолда GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилган. GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y кўринишдаги шифрлаш алгоритмларида ГОСТ 28147–89 шифрлаш алгоритмининг раунд акслантиришларидан тўлиқ фойдаланилган бўлса, GOST28147–89–

RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y кўринишдаги шифрлаш алгоритмларда эса S–блокларда ўрнига қўйиш ва чапга циклик суриш акслантиришлари қўлланилган. Барча шифрлаш алгоритмлари калит узунлиги 256 битдан 1024 битгача 128 бит қадам билан ўзгаради. GOST28147–89–IDEA4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, GOST28147–89–IDEA16–2, GOST28147–89–RFWKIDEA16–2, GOST28147–89–PES16–2, GOST28147–89–RFWKPES16–2 шифрлаш алгоритмлари блок узунлиги 128 битга, қолган шифрлаш алгоритмлари блок узунлиги 256 битга тенг. GOST28147–89–IDEA16–2, GOST28147–89–RFWKIDEA16–2, GOST28147–89–PES16–2, GOST28147–89–RFWKPES16–2 шифрлаш алгоритмлари қисм блоклари узунлиги 8 битга тенг ва қолган бошқа алгоритмлар қисм блоклари узунлиги 32 битга тенг. Шифрлаш алгоритмларнинг тезликлари 4–жадвалда келтирилган.

4–жадвал

Шифрлаш алгоритмлари тезликлари (Мбайт/с)

Шифрлаш алгоритмлари	8 раунд	12 раунд	14 раунд
ГОСТ 28147–89 (32 раунд)	≈27.855		
GOST28147–89–IDEA4–2	≈40.029	≈29.069	≈22.123
GOST28147–89–RFWKIDEA4–2	≈40.145	≈30.228	≈22.883
GOST28147–89–PES4–2	≈40.029	≈29.069	≈22.123
GOST28147–89–RFWKPES4–2	≈40.145	≈30.228	≈22.883
GOST28147–89–IDEA8–4	≈40.015	≈29.047	≈22.059
GOST28147–89–RFWKIDEA8–4	≈40.137	≈30.103	≈22.819
GOST28147–89–PES8–4	≈40.015	≈29.047	≈22.059
GOST28147–89–RFWKPES8–4	≈40.137	≈30.103	≈22.819
GOST28147–89–IDEA16–2	≈33.783	≈24.691	≈18.315
GOST28147–89–RFWKIDEA16–2	≈33.846	≈24.813	≈18.867
GOST28147–89–PES16–2	≈33.783	≈24.691	≈18.315
GOST28147–89–RFWKPES16–2	≈33.846	≈24.813	≈18.867

Шифрлаш алгоритмларининг S–блоклари параметрлари ҳисобланган бўлиб, $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC=2, BIC=4. Шифрлаш алгоритмлари учун қуйидаги тасдиқ ўринли:

Тасдиқ 6. GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари S–блоклари умумий мураккаблик кўрсаткичи S^4_{index}=0,8916, яъни ГОСТ 28147–89 шифрлаш алгоритми умумий мураккаблик кўрсаткичидан юқори.

GOST28147–89–IDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–RFWKPES4–2 шифрлаш алгоритмларининг исталган блокидаги ўзгариши кўпи билан икки раунддан сўнг, қолган барча шифрлаш алгоритмларида эса кўпи билан уч раунддан сўнг таъсир этади.

Шунингдек, барча шифрлаш алгоритмларда калитнинг битта бити ўзгариши биринчи раунддан сўнг барча блокларга таъсир этади.

Шифрлаш алгоритмларига чизиқли криптотаҳлил усули қўлланилди. Криптотаҳлил усули қўллаш жараёнида майдонда кўпайтириш амали ўрнига қўшиш амали фойдаланилди ва биринчи раундгача, чиқувчи акслантиришдан сўнг қўлланиган амаллар ҳисобга олинмади. Ҳисоблаш натижалари 5–жадвалда келтирилган.

5–жадвал

Чизиқли криптотаҳлил усули натижалари

Шифрлаш алгоритмлари	4 раунд	8 раунд	12 раунд
GOST28147–89–IDEA4–2	2^{35}	2^{70}	2^{104}
GOST28147–89–PES4–2	2^{35}	2^{70}	2^{104}
GOST28147–89–RFWKIDEA4–2	2^{27}	$2^{54.5}$	2^{81}
GOST28147–89–RFWKPES4–2	2^{27}	$2^{54.5}$	2^{81}
GOST28147–89–IDEA8–4	2^{83}	–	–
GOST28147–89–PES8–4	2^{83}	–	–
GOST28147–89–RFWKIDEA8–4	2^{75}	–	–
GOST28147–89–RFWKPES8–4	2^{75}	–	–
GOST28147–89–IDEA16–2	2^{51}	2^{102}	–
GOST28147–89–PES16–2	2^{51}	2^{102}	–
GOST28147–89–RFWKIDEA16–2	2^{43}	2^{86}	–
GOST28147–89–RFWKPES16–2	2^{43}	2^{86}	–

Жадвалдан кўриниб турибдики, кўпайтириш амали ўрнига қўшиш амали фойдаланилгани ва биринчи раундгача қўлланиган амаллар ҳисобга олинмаган тақдирда ҳам шифрлаш бардошлиги нисбатан юқори.

ХУЛОСА

«Ягона алгоритмга асосланган функционал Лай–Месси тармоғи назарияси ва амалиёти» мавзусидаги докторлик диссертацияси бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Раунд функциялардан ташкил топган IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y (X–қисм блоклар сони, Y–раунд функциялар сони) кўринишдаги Лай–Месси тармоқлари ишлаб чиқилди. Тармоқларда шифрлаш ва дешифрлашда битта алгоритмдан фойдаланиши исботланди.

2. Ишлаб чиқилган тармоқлар блоклари сони тўртта, саккизта, ўн олтита, ўттиз иккита ва 2m та бўлиб, қисм блоклари узунликлари 8, 16 ва 32 битга тенг бўлиб, IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y кўринишдаги тармоқлар раунд функциялари сифатида узунлиги 8, 16 ва 32 бит бўлган битта, иккита, тўртта, саккизта, ўн олтита, ўттиз иккита ва *m* та кириш ва чиқиш қисм блокларга эга акслантиришлар олинади, тармоқ асосида қисм блоклари узунликлари 8, 16 ва 32 битга тенг бўлганда блок

узунлиги 8X, 16X ва 32X бит бўлган шифрлаш алгоритмларини яратиш имконини беради.

3. Ниберг конструкцияси асосида ишлаб чиқилган ўлчами 4x4, 8x8 бўлган бардошли S–блоклар янги блокли шифрлаш алгоритмларини яратишда хизмат қилади.

4. AES шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида AES–IDEAX–Y, AES–RFWKIDEAX–Y, AES–PESX–Y, AES–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилди. Шифрлаш алгоритмлари тезликлари ва бардошлиги AES шифрлаш алгоритмидан юқори. Шифрлаш алгоритмлари раундлар сони 10, 12, 14 га тенг бўлиб, калит узунлиги 256 битдан 1024 битгача ўзгаради. Маълумот махфийлиги ва шифрлаш тезлигига боғлиқ ҳолда раундлар сони ва калит узунлигини танлаб олиши имконини беради. Алгоритмларни қўллаш тезликни 16–38% оширишга олиб келади ва чизиқли криптотаҳлил усулига бардошлиги 60% гача ошади.

5. ГОСТ 28147–89 шифрлаш алгоритми раунд функциясини Лай–Месси тармоқлари раунд функцияси сифатида қўллаш натижасида GOST28147–89–IDEAX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKPESX–Y кўринишдаги шифрлаш алгоритмлари ишлаб чиқилди. Шифрлаш алгоритмлари раундлар сони 8, 12, 16 га тенг бўлиб, калит узунлиги 256 битдан 1024 битгача ўзгаради. Маълумот махфийлиги ва шифрлаш тезлигига боғлиқ ҳолда раундлар сони ва калит узунлигини танлаб олиши имконини беради.

6. Барча 8–раундли алгоритмларнинг ва 12–раундли GOST28147–89–IDEA4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, GOST28147–89–IDEA8–4, GOST28147–89–RFWKIDEA8–4, GOST28147–89–PES8–4, GOST28147–89–RFWKPES8–4 шифрлаш алгоритмларининг тезлиги ГОСТ 28147–89 шифрлаш алгоритмининг тезлигидан юқори. Шифрлаш алгоритмлари бардошлиги ГОСТ 28147–89 шифрлаш алгоритмидан юқори. Алгоритмларни қўллаш чизиқли криптотаҳлил усулига бардошликни 60% гача оширишга, баъзи ҳолатларда эса тезликни оширишга хизмат қилади.

НАУЧНЫЙ СОВЕТ DSc.27.06.2017.FM.01.02 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ НАЦИОНАЛЬНОМ УНИВЕРСИТЕТИ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТИ УЗБЕКИСТАНА

ТУЙЧИЕВ ГУЛОМ НУМОНОВИЧ

ТЕОРИЯ И ПРАКТИКА ФУНКЦИОНАЛЬНОЙ СЕТИ ЛАЙ–МЕССИ, ОСНОВАННАЯ НА ЕДИНОМ АЛГОРИТМЕ

05.01.05–Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ ДОКТОРСКОЙ ДИССЕРТАЦИИ (DSc) ПО ФИЗИКО–МАТЕМАТИКИЧЕСКИМ НАУКАМ

Ташкент–2017

Тема диссертациии зарегистрирована за № B2017.1.DSc/FM3 в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан.

Диссертация выполнена в Национальном университете Узбекистана.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб–странице научного совета (www.nuu.uz) и образовательной информационной сети «ZIYONET» (www.ziyonet.uz)

Научный консультант:	**Арипов Мирсаид Мирсидикович** доктор физико–математических наук, профессор
Официальные оппоненты:	**Каримов Маджит Маликович** доктор технических наук, профессор
	Касимов Надимулло Хабибуллаевич доктор физико–математических наук, профессор
	Утеулиев Ниетбай Утеулиевич доктор физико–математических наук, профессор
Ведущая организация:	**ГУП «UNICON.UZ»**

Защита диссертации состоится «__» _____2017 г. в ___ часов на заседании научного совета DSc.27.06.2017.FM.01.02 при Национальном университети Узбекистана (Адрес: 100174, Ташкент, ВУЗ Городок, ул. Университет–4. Тел.:(99871) 246–02–24; факс:(99871) 246–53–21; e–mail: info@nuu.uz).

С докторской диссертацией можно ознакомиться в Информационно–ресурсном центре Национального университета Узбекистана (регистрационный номер __). (Адрес: 100174, Ташкент, ВУЗ Городок, ул. Университет–4. Тел.:(99871) 246–02–24; факс:(99871) 246–53–21; e–mail: info@nuu.uz).

Автореферат диссертации разослан «___» _____ 2017 года.
(протокол рассылки № __ от « » _____2017 г.).

А.Р.Марахимов
Председатель научного совета
по присуждению учёной степени, д.т.н

З.Р.Рахмонов
Ученый секретарь научного совета
по присуждению учёной степени, д.ф.–м.н.

Р.Д.Алоев
Председатель научного семинара при
Научном совете по присуждению
учёной степени, д.ф.–м.н.

ВВЕДЕНИЕ (аннотации диссертации доктора наук (DSc))

Актуальность и востребованность темы диссертации. В мире направлении криптографии занимает важное место в сфере обеспечения информационной безопасности. «Роль криптографии в защите информации возрастает в связи с расширением областей ее применения, затрагивающих интересы многих людей»[3]. С бурным развитием информационных технологий в мире возрастает необходимость в защите информации и для этой цели ведутся широкомасштабные исследования. В настоящее время криптографические алгоритмы стали неотъемлемой частью операционных систем и растет потребность в их широком внедрении в процессы передачи, хранения и обработки информации. В связи с этим одной из актуальных проблем считается разработка сетей, использующих один и тот же алгоритм при зашифровании и расшифровании, алгоритмов шифрования на их основе, а также разработка стойких S–блоков. В мире достигли определенных успехов в области разработки блочных алгоритмов шифрования, S–блоки, где одним из важнейшей задач становится разработка сетей, использующие один и тот же алгоритм при зашифровании и расшифровании, алгоритмов шифрования на основе сетей, а также стойких S–блоков.

За годы независимости в нашей стране эффективному развитию в сфере криптографии и разработке стойких алгоритмов шифрования было уделено особое внимание. В частности, в стратегии действий Республики Узбекистан отдельное внимание уделено на совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере. В этой сфере, проведены ряд исследований и достигнуто значительным успехам, в сфере разработки стойких алгоритмов шифрования, созданию программных и программно–аппаратных средств алгоритмов шифрования, функциональных сетей Фейстеля, методов оценки стойкости криптографических преобразований.

В мировой практике особое значение приобретает создание сетей использующие один и тот же алгоритм при зашифровании и расшифровании, и состоящие из раундовой функции, алгоритмов шифрования на основе этих сетей и разработка стойких S–блоков для них. В этой сфере одним из важнейших задач считается проведение целевых научных исследований, в частности, особое внимание обращается на разработку сетей, в которых при зашифровании и расшифровании используют один и тот же алгоритм, и алгоритмов шифрования на их основе, оценке стойкости алгоритмов шифрования, а также созданию стойких S–блоков.

Данное диссертационное исследование в определенной мере служит выполнению задач, обозначенных в Постановлении Президента Республики

[3] Ростовцев А.Г. Алгебраическое основы криптографии, 2000 г.

Узбекистан от 3 апреля 2007 года №ПП–614 «О мерах по организации криптографической защиты информации в Республике Узбекистан», Постановлении Кабинета Министров Республики Узбекистан от 21 ноября 2007 года №242 «Об утверждении Положения о лицензировании деятельности по проектированию, производству, реализации, ремонту и эксплуатации криптографических средств защиты информации», Указ Президента Республики Узбекистан от 7 февраля 2017 года №УП–4947 «О Стратегии Действий По Дальнейшему Развитию Республики Узбекистан», а также в других нормативно–правовых документах, связанных с указанной деятельностью.

Соответствие исследования с приоритетными направлениями развития науки и технологий республики. Настоящая диссертационная работа выполнена в рамках приоритетных направлений развития науки и технологий республики IV. «Информатизация и развитие информационно–коммуникационных технологий».

Обзор зарубежных научно–исследовательских работ по теме диссертации[4]. Научные исследования, направленные на разработку сетей, использующих один и тот же алгоритм при зашифровании и расшифровании, оценку стойкости алгоритмов шифрований AES, ГОСТ 28147–89, IDEA, PES, разработку S–блоков и совершенствование методов оценки их стойкости, проводятся в ведущих научных центрах и высших образовательных учреждениях мира, в том числе в Bar Ilan University, University of Haifa, Tel Aviv University, Weizmann Institute (Израиль), Katholieke University Leuven (Бельгия), Академии криптографии, Московском государственном университете, Южном федеральном университете (Россия), University of Luxembourg (Люксембург), Dian Ji University, Jiaotong University (Хитой), Swiss Federal Institute of Technology (Швейцария), Vienna Technical University (Австрия), Lyon University (Франция), University College London (Англия), University of California, Conterpane Internet Security (АҚШ), Indian Statistical Institute (Ҳиндистон), Korea University (Корея), Nanyang Technological University (Сингапур), Национальном университете Узбекистана, Ташкентском университете информационных технологий, ГУП «UNICON.UZ» (Узбекистан) и др.

В результате проведенных в разных странах мира исследований по применению методов криптоанализа к алгоритмам шифрования PES, IDEA, AES и ГОСТ 28147–89, разработке сетей использующие один и тот же алгоритм при зашифровании и расшифровании и стойких S–блоков был получен ряд положительных научных результатов, в том числе: к 6.5 и 7 раундовым алгоритмам шифрования IDEA применен метод криптоанализа Related key rectangle и определено, что для 7 раундового алгоритма шифрования требуется 2^{65} пар открытого текста–шифртекста (Bar Ilan

[4] Обзор зарубежных научных исследований по теме диссертации проведен на основе нижеприведенных и других источников Южный федеральный Университет, University of Haifa, Swiss Federal Institute of Technology, Katholieke University Leuven, Indian Statistical Institute, University of California, University of York и др.

University, University of Haifa, Tel Aviv University, Израиль); к 7 раундовому алгоритму шифрования PES применен метод диференциального криптоанализа и выяснено, что требуется 2^{64} пар открытого текста–шифртекста (Swiss Federal Institute of Technology in Zurich, Швейцария); к 7 и 8 раундовым алгоритмам шифрования AES–128, AES–192, AES–256 применен метод криптоанализа Impossible Differential и установлено, что требуется более 2^{91} пар открытого текста–шифртекста (Bar Ilan University, University of Haifa, Израиль); к алгоритму шифрования ГОСТ 28147–89 применен алгебраический метод криптоанализа, получены уравнения для S–блоков и решены методом XSL, в результате установлено, что требуется 2^{38} пар открытого текста–шифртекста (Южный федеральный университет, Россия); разработаны сеть Фейстеля, ее усовершенствованный вид, расширенная сеть Фейстеля (IBM, Conterpane Internet Security, University of California, США), схема Лай–Месси и ее расширенный вид (Swiss Federal Institute of Technology, Швейцария, Dian Ji University, Jiaotong University, Китай); созданы методы генерации S–блоков с высокой нелинейностью и алгебраической степенью нелинейности (Vienna Technical University, Katholieke Universite Leuven, Бельгия); созданы методы генерации бульевых функций с высокой нелинейностью (Indian Statistical Institute, Индия, University of Science and Technology of China, Китай, University of Alabama, США).

В мире в рамках разработки сетей использующих один и тот же алгоритм при зашифровании и расшифровании, алгоритмов шифрования на основе этих сетей, генерации стойких S–блоков, а также оценке стойкости алгоритмов шифрования ведутся исследования по ряду приоритетных направлений, в том числе: усовершенствование существующих сетей использующий один и тот же алгоритм при зашифровании и расшифровании; разработке алгоритмов шифрования на основе этих сетей; создание методов генерации стойких S–блоков для алгоритмов шифрования; оценке стойкости алгоритмов шифрования; создание методов генерации бульевых функций с высокой нелинейностью.

Степень изученности проблемы. В настоящее время вопросы анализа схемы Лай–Месси, использующей один и тот же алгоритм при зашифровании и расшифровании, разработка на основе схемы алгоритмов шифрования рассмотрены в научных трудах ряда ученых: E.Biham, O.Dunkellman, Z.Gong, P.Junod, N.Keller, X.Lai, J.Lee, Y.Luo, M.Macchetti, J.Massey, J.Nakahara, J.Park, B.Preneel, J.Rijmen, S.Vaudenay, J.Vandewalle, Z.Wu, A.Yun, М.Арипов, М.Бондаренко, И.Горбенко, В.Долгов, Р.Олейников, В.Руженцев и других.

Вопросам анализа алгоритмов шифрования AES, ГОСТ 28147–89, оценки стойкости методами криптоанализа, генерации S–блоков с высокой алгебраической нелинейностью и бульевых функций посвящены работы M.Aref, B.Bahrak, A.Canteaunt, C.Carlet, P.Charpin, J.Clark, N.Courtois, I.Dinur, O.Dunkelman, D.Feng, N.Ferguson, C.Fontaine, H.Gilbert, G.Ivanov, J.Jacob, S.Kavut, N.Keller, J.Kelsey, J.Kim, S.Lucks, J.Lu, S.Maitra, M.Minier,

W.Millan S.Nikova, N.Nikolov, K.Nyberg, B.Schneier, A.Shamir, M.Stay, P.Stanica, S.Stepney, S.Sung, D.Wagner, D.Whiting, W.Wu, M.Yusel, W.Zhang, X.Zhang, Б.Абдурахимов, Л.Бабенко, Е.Маро, В.Рудской и других ученых, которые достигли определенных положительных результатов.

Вместе с тем, недостаточно исследованы вопросы создания сети использующие один и тот же алгоритм при зашифровании и расшифровании, алгоритмов шифрования на основе данной сети, разработки стойких S–блоков.

Связь темы диссертации с научно–исследовательскими работами высшего образовательного учреждения, где выполнена диссертация. Диссертационная работа выполнена в рамках проекта на тему «Актуальные проблемы прикладной математики и информационных технологий» (2012–2016) Национального университета Узбекистана.

Целью исследования является разработка сети Лай–Месси, новых алгоритмов шифрования на основе этой сети и генерация стойких S–блоков.

Задачи исследования:

анализ схемы Лай–Месси, алгоритмов шифрования IDEA, PES, AES, ГОСТ 28147–89, а также свойств бульевых функций, применяемых при оценке стойкости S–блоков;

разработка сетей Лай–Месси, использующих один и тот же алгоритм при зашифровании и расшифровании и состоящих из раундовых функций;

разработка стойких S–блоков размером 8x8, 4x4 на основе конструкции Ниберга;

создание новых алгоритмов шифрования в результате применения раундовых функций алгоритмов шифрования AES и ГОСТ 28147–89 в качестве раундовых функций сети Лай–Месси;

оценка стойкости разработанных алгоритмов шифрования.

Объектом исследования является сети Лай–Месси, конструкция Ниберга.

Предметы исследования составляют новые алгоритмы шифрования, разработанные в результате применения раундовых функций алгоритмов шифрования AES и ГОСТ 28147–89 в качестве раундовых функций сети Лай–Месси, методы генерации S–блоков и бульевых функций.

Методы исследования. Результаты диссертации получены на основе методов системного и прикладного программирования, прикладной криптографии с использованием комбинаторики, математической логики, теории вероятностей. В методах разработки новых алгоритмов шифрования, стойких S–блоков, бульевых функций применена технология программирования.

Научная новизна исследования заключается в следующем:

созданы сети Лай–Месси в виде IDEAX–Y, RFWKIDEAX–Y с использованием структуры алгоритма шифрования IDEA и схемы Лай–Месси;

созданы сети Лай–Месси в виде PESX–Y, RFWKPESX–Y с использованием структуры алгоритма шифрования PES и схемы Лай–Месси;

разработаны алгоритмы шифрования в виде AES–IDEAX–Y, AES–RFWKIDEAX–Y, AES–PESX–Y, AES–RFWKPESX–Y в результате применения раундовой функции алгоритма шифрования AES в качестве раундовых функций сетей Лай–Месси;

разработаны алгоритмы шифрования в виде GOST28147–89–IDEAX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKPESX–Y в результате применения раундовой функции алгоритмов шифрования ГОСТ 28147–89 в качестве раундовых функций сетей Лай–Месси;

на основе конструкции Ниберга разработаны стойкие S–блоки размером 8x8, 4x4.

Практические результаты исследования заключаются в следующем:

разработаны сети Лай–Месси в виде IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y;

на основе конструкции Ниберга разработаны стойкие S–блоки размером 8x8, 4x4 и их программное обеспечение;

за счет применения преобразований алгоритмов шифрования AES и ГОСТ 28147–89 в качестве раундовых функций сетей Лай–Месси разработаны новые алгоритмы шифрования и их программное обеспечение.

Достоверность результатов исследования. Достоверность результатов исследования доказаны путем строгого сравнения результатов вычислительных экспериментов на основе общепризнанных критериев и подтверждены количественными результатами исследования. Создано и апробировано программное обеспечение всех алгоритмов шифрования и методов разработки S–блоков, бульевых функций.

Научная и практическая значимость результатов исследования. В качестве научной значимости результатов исследования служат методы разработки сети Лай–Месси, а также стойких S–блоков и бульевых функций на основе конструкции Ниберга.

Практическая значимость полученных результатов исследования заключается в том, что новые стойкие и высокоскоростные алгоритмы шифрования, за счет применения раундовых преобразований алгоритмов шифрования AES и ГОСТ 28147–89 в качестве раундовых функций сетей Лай–Месси, могут быть широко использованы для защиты информации в процессе передачи и хранения, а стойкие S–блоки – в разработке блочных алгоритмов шифрования.

Внедрение результатов исследования. На базе сети Лай–Месси, основанной на едином алгоритме:

алгоритм шифрования AES–IDEA32–4 созданный с использованием раундовых преобразований алгоритмов шифрования AES, реализованы в программном обеспечении «Himfayl» в защите файлов через шифровании в ГУП «UNICON.UZ» (справка Министерства по развитию информационных

технологий и коммуникаций от 29 мая 2017 года №33–8/3256). Наличие возможности выбора длины ключа и количества раундов в алгоритме шифрования AES–IDEA32–4, а также применение алгоритмов шифрования в защите файлов произвольного формата привели к росту скорости шифрования на 17%.

алгоритм шифрования GOST28147–89–IDEA16–2 созданный с использованием раундовых преобразований алгоритма шифрования ГОСТ 28147–89, использован в системе «Himfayl» ГУП «UNICON.UZ» в целях обеспечение безопасности файлов произвольного формата (справка Министерства по развитию информационных технологий и коммуникаций от 29 мая 2017 года №33–8/3256). Наличие возможности выбора длины ключа и количества раундов в алгоритме шифрования GOST28147–89–IDEA16–2, а также применение алгоритмов шифрования в защите файлов произвольного формата привели к росту скорости шифрования на 21%.

Из результатов диссертации алгоритмы шифрования AES–PES16–1, AES–RFWKPES16–1, AES–RFWKPES32–1, AES–RFWKIDEA32–1 в ведущих зарубежных научных работах (International Journal of Network Security, vol.19, No.6, pp.899–903, Nov. 2017; International Journal of Network Security, vol.19, No.6, pp.984–994, Nov. 2017; International Journal of Network Security, vol.19, No.3, pp.413–420, May 2017; Displays, vol.49, pp.116–123, Sep. 2017) использованы для создание криптографического моделя на основе симметричных алгоритмов. Применение научных результатов позволяет при построении дальнейшие характеристики H–вектора, скрытии информации в бинарных изображениях, при защите изображении больших размеров, при создании криптографического моделя для эффективного использовании нескольких ключевых слов на основе зашифрованных данных.

Апробация результатов исследования. Результаты исследования обсуждены на 6 международных и 7 республиканских научно–практических семинарах и конференциях.

Опубликованность результатов исследования. По теме диссертации опубликованы всего 50 научных работ, в т.ч. 21 статей (13 в республиканских и 8 в зарубежных журналах) опубликованы в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для основных научных результатов докторских диссертаций. Получены 6 свидетельств о регистрации программных средств для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 198 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обосновывается актуальность и востребованность темы диссертации, в соответствии с исследованиям приоритетных направлений

развития науки и технологий республики, формулируются цель и задачи, а также объект и предмет исследования, изложена научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта теоритическая и практическая значимость полученных результатов, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работ и структура диссертации.

В первой главе диссертации **«Анализ схемы Лай–Месси и генерация S–блоков, булевых функций на основе конструкции Ниберга»** проанализированы схемы Лай–Месси, алгоритмы шифрования PES ва IDEA основанные на этой схеме, приведены результаты методов криптоанализа примененных к алгоритмам шифрования. Приведены методы генерации S–блока и булевых функций на основе конструкции Ниберга, проанализированы преобразования алгоритмов шифрования AES ва ГОСТ 28147–89, которые использованы при создании новых алгоритмов шифрования.

Процессы зашифрования и расшифрования *n*–раундовая схема Лай–Месси приведены на рис. 1 и 2. Пусть *F*–раундовая функция, *H*–преобразование и K_0, K_1, ..., K_n раундовые ключи. Блок открытого текста делится на части L_0 и R_0. В каждом раунде преобразование осуществляется следующим образом:

$$(L'_{i+1}, R'_{i+1}) = H(L'_i + T_i, R'_i + T_i),$$

где $T_i = F(L'_i - R'_i, K_i)$ и $(L'_i, R'_i) = H(L_0, R_0)$. В качестве шифртекста выбираются значения $(L_{n+1}, R_{n+1}) = (L'_{n+1}, R'_{n+1})$.

На сети Фейстеля и схем Лай–Месси шифрование осуществляеться следующим образом:

Сеть Фейстеля	Схемы Лай–Месси
1. $L_0 \leftarrow x_L$, $R_0 \leftarrow x_L$,	1. $\alpha_0 \leftarrow x_L$, $\beta_0 \leftarrow x_L$,
2. $L_{i+1} \leftarrow R_i$, $R_{i+1} \leftarrow L_i \oplus F(R_i)$,	2. $\alpha_{i+1} \leftarrow \alpha_i + F(\alpha_i - b_i)$, $\beta_{i+1} \leftarrow \beta_i + F(\alpha_i - \beta_i)$,
3. $y_L \leftarrow L_n$, $y_R \leftarrow R_n$.	3. $y_L \leftarrow \alpha_n$, $y_R \leftarrow \beta_n$.

В схеме Лай–Месси, как и у сети Фейстеля, при зашифровании и расшифровании используется один и тот же алгоритм, только раундовые ключи применяются в обратном порядке и требуется вычислить преобразование H^{-1}.

Для того, чтобы схема Лай–Месси была псевдохаотичной (pseudorandomness) достаточны три, а для сильно псевдохаотичной схемы достаточны четыре раунда. Таким образом, для построения псевдослучайной перестановки из псевдослучайной функции достаточно трех, а для сильно псевдослучайной перестановки достаточно четырех раундовых схем Лай–Месси.

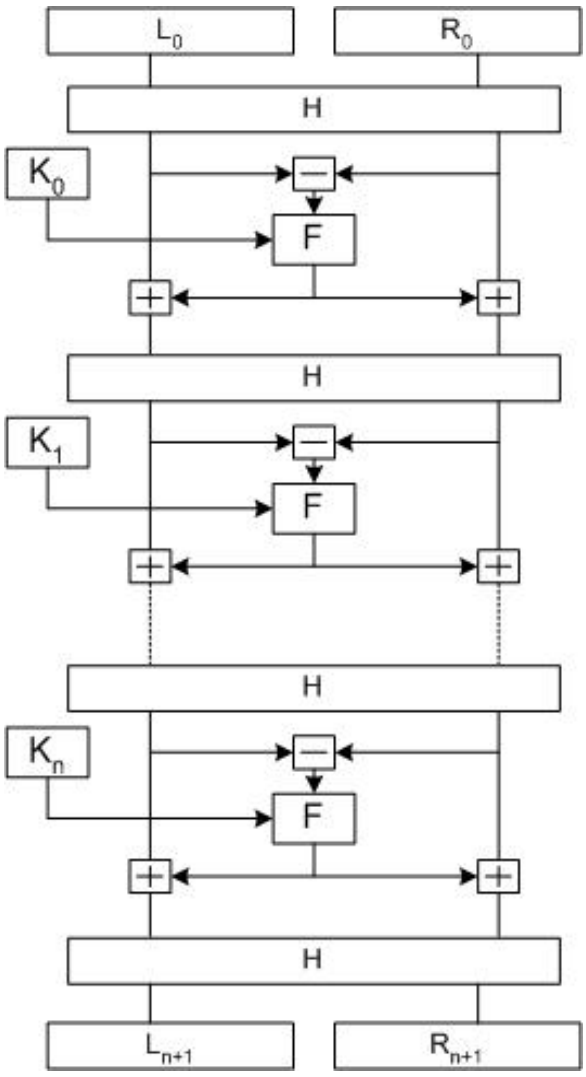


Рис. 1. Процесс зашифрования *n*–раундовой схемы Лай–Месси

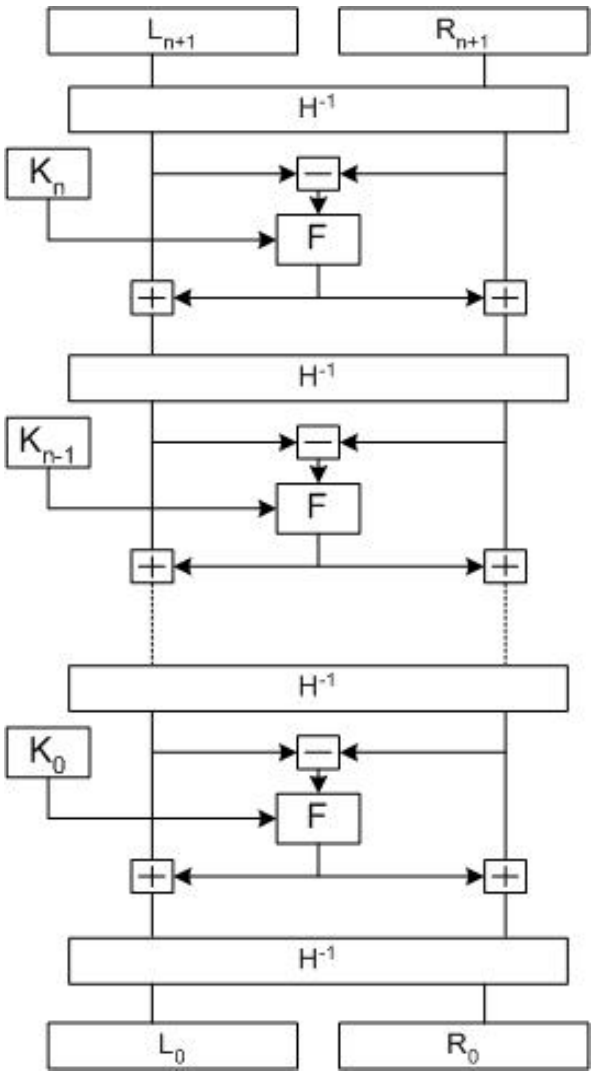


Рис. 2. Процесс расшифрования *n*–раундовой схемы Лай–Месси

После чего, проработан алгоритм шифрования PES и назван IPES (Improved PES). В 1992 году алгоритм шифрования IPES переименовали на IDEA (International Data Encryption Algorithm). Длина ключа алгоритма равна 128 битам и длина блока 64 битам, состоит из 8 раундов и выходного преобразования. До сих пор алгоритм шифрования IDEA не утратил свое значение и применяеться на практике. К алгоритмам шифрования применены несколько методов криптоанализа, результаты приведены в 1 и 2–таблицах.

1–таблица

Результаты криптоанализа, применённых к алгоритму шифрования PES

Тип атак	Число раундов	Количество выбранных текстов	Затраченное время (число операции)
Differential	7	2^{64}	2^{160}
SQUARE	2.5	2^{17}	2^{47}
SQUARE	2.5	2^{32}	2^{63}
Related–Key SQUARE	2.5	2	2^{41}

2–таблица

Результаты криптоанализа, применённых к алгоритму шифрования IDEA

Тип атак	Число раундов	Количество выбранных текстов	Затраченное время (число операции)
Differential	2.5	2^{10}	2^{106}
SQUARE	2.5	2^{48}	2^{79}
Differential–Linear	3	2^{30}	2^{44}
Differential	3	2^{30}	$0.75 * 2^{44}$
Truncated Differential	3.5	2^{56}	2^{67}
Miss–in–the–middle	4	2^{37}	2^{70}
Related–Key Differential–Linear	4	$2^{38.3}$	–
Miss–in–the–Middle	4.5	2^{64}	2^{112}
Meet–in–the–middle	5	2^{24}	2^{126}
Linear	5	2^{19}	2^{103}
Higher–order Differential–Linear	5.5	2^{32}	2^{114}
Higher–order Differential–Linear	6	2^{64}–2^{52}	$2^{126.85}$
Related key rectangle	7	2^{65}	$2^{104.2}$

S–блоки алгоритма шифрования AES разработаны на основе конструкции Ниберга. Конструкции Ниберга представляют собой отображение в виде мультипликативных обратных элементов в поле Галуа $GF(2^k)$ $y = x^{-1} \bmod[f(z), p]$, $x, y \in GF(2^k)$ скомбинированных с аффинным преобразованием $b = A \cdot y + a$, $a, b \in GF(2^k)$, где $f(z) = z^8 + z^4 + z^2 + z + 1$– неприводимый полином над полем *GF(2)*, *A*–невырожденная матрица размера $k \times k$, *a*–вектор сдвига, *p*–2–характеристика расширенного поля Галуа, и принято, что 0^{-1}=0.

А для генерации S–блоков размером 8x8 конструкция Ниберга обобщена в виде *GenerSBox(m,b)* следующим образом:

$$\begin{pmatrix} s_7 \\ s_6 \\ s_5 \\ s_4 \\ s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 \\ m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 & m_5 \\ m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 & m_4 \\ m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 & m_3 \\ m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 & m_2 \\ m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 & m_1 \\ m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_0 \end{pmatrix} \begin{pmatrix} c_7 \\ c_6 \\ c_5 \\ c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \oplus \begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

здесь $b=(b_0,b_1,b_2,b_3,b_4,b_5,b_6,b_7)$, $m=(m_0,m_1,m_2,m_3,m_4,m_5,m_6,m_7)$, $s=(s_0,s_1,s_2,s_3,s_4,s_5,s_6,s_7)$, $c=(c_0,c_1,c_2,c_3,c_4,c_5,c_6,c_7)$ и a–входное значение преобразования, s–выходное значение преобразования, $c=a^{-1}$. Если m и b принимает постоянное значение и значение a изменяется от нуля до 255, то формируется S–блок размером 8x8, то есть $S_{8x8}=GenerSBox(m,b)$. В качестве S–блока алгоритма шифрования AES можно выбирать преобразование $GenerSBox(241,99)$. Для S–блока алгоритма шифрования выполняется условие $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, $Dd_j(S)=8$, $1\le j\le 8$.

Для генерации S–блоков размером 4x4 конструкция Ниберга обобщена в виде $GenerSBox(m^0,m^1,m^2,m^3,b)$ следующим образом:

$$\begin{pmatrix} s_3 \\ s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} m_0^0 & m_1^0 & m_2^0 & m_3^0 \\ m_0^1 & m_1^1 & m_2^1 & m_3^1 \\ m_0^2 & m_1^2 & m_2^2 & m_3^2 \\ m_0^3 & m_1^3 & m_2^3 & m_3^3 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \oplus \begin{pmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

здесь c_i и s_i–соответственно i–бит входного и выходного значения и $s=(s_0,s_1,s_2,s_3)$, $c=(c_0,c_1,c_2,c_3)$, $b=(b_0,b_1,b_2,b_3)$, $m^0=(m_0^0,m_1^0,m_2^0,m_3^0)$, $m^1=(m_0^1,m_1^1,m_2^1,m_3^1)$, $m^2=(m_0^2,m_1^2,m_2^2,m_3^2)$, $m^3=(m_0^3,m_1^3,m_2^3,m_3^3)$, $c=a^{-1}$. Если m^0, m^1, m^2, m^3, b–константа и переменная a измеряется от нуля до 15, то генерируется S–блок размера 4x4.

На основе конструкции Ниберга

– создан метод генерации S–блоков размером 8x8 и программное обеспечение, для S–блоков выполняется условие $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, SAC=8, BIC=8, число S–блоков равно 32640.

– создан метод генерации булевых функций, состоящий из восьми переменных. Для булевых функции выполняется условие $NL(f)=112$, $\deg(f)=7$, $Dd_j(f)\le 8$ $(1\le j\le 8)$. Число булевых функций равно 256 и на основе генерированных булевых функций можно создать S–блоки, для S–блоков выполняется условие $NL(S)=112$, $\deg(S)=7$, $\lambda_F=32/256$, $\delta_F=4/256$, SAC=8, BIC=8;

– создан метод генерации S–блоков размером 4x4 и программное обеспечение. Для S–блоков выполняется условие $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC≤2, BIC≤4, число S–блоков равно 221760;

– создан метод генерации булевых функций, состоящий из четырех переменных. Для булевых функции выполняется условие $NL(f)=4$, $\deg(f)=3$, $Dd_j(f)\le 4$, $1\le j\le 4$, число булевых функции равно 28 и на основе генерированных булевых функций можно создать S–блоки. Для S–блоков выполняется условие $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC≤2, BIC≤4, BIC≤4, число S–блоков равно 236544.

Для конструкции Ниберга имеют место следующие два утверждения:

Утверждение 1. На основе конструкции Ниберга вида *GenerSBox(m,b)* сгенерировано 32640 стойких S–блоков размером 8x8 и 256 булевых функций.

Утверждение 2. На основе конструкции Ниберга вида *GenerSBox(m^0,m^1,m^2,m^3,b)* сгенерировано 221760 стойких S–блоков размером 4x4 и 28 булевых функций.

Для вычислении стойкости S–блока используется общий показатель сложности. Общий показатель сложности при n=8 определено следующим образом:

$$S^8_{index} = \frac{\frac{\deg(F)}{7} + \frac{NL(F)}{118} + \frac{258 - \max XOR(a,b)}{256} + \frac{64 - SAC}{64} + \frac{64 - BIC}{64}}{5}$$

При n=4 общий показатель сложности определено следующим образом:

$$S^4_{index} = \frac{\frac{\deg(F)}{3} + \frac{NL(F)}{4} + \frac{18 - \max XOR(a,b)}{16} + \frac{16 - SAC}{16} + \frac{16 - BIC}{16}}{5}$$

Теорема 1. Общий показатель сложности S–блока $0<S^8_{index}<1$, $0<S^4_{index}<1$ и для идельного S–блока выполняется $S^8_{index}=1$, $S^4_{index}=1$.

Для алгоритмов шифрования ГОСТ 28147–89 и AES имеют место следующие утверждения:

Утверждение 3. Первый и четвертый S–блоки алгоритма шифрования ГОСТ 28147–89 S^4_{index}=0,8, нолевой S–блок S^4_{index}=0,8083, второй S–блок S^4_{index}=0,775, третий и седмой S–блок S^4_{index}=0,6833, пятий S–блок S^4_{index}=0,75, шестой S–блоки S^4_{index}=0,7083.

Утверждение 4. S–блок алгоритма шифрования S^8_{index}=0,9382.

Во второй главе диссертации **«Сети Лай–Месси вида IDEAX–Y, RFWKIDEAX–Y, разработанные на основе структуры алгоритма шифрования IDEA и схем Лай–Месси»** приведены сети Лай–Месси вида IDEAX–Y, RFWKIDEAX–Y, созданные с использованием структуры алгоритма шифрования IDEA и схемы Лай–Месси, здесь X–число подблоков, Y–число раундовых функций. Основным преимуществом этих сетей является то, что при шифровании и дешифровании используется один и тот же алгоритм и в качестве раундовой функции сети можно использовать любые преобразования.

Схема сети IDEA4–2 приведена на рис. 3, длина подблоков X_0, X_1, X_2, X_3, раундовые ключи $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i=\overline{1...n+1}$, входные и выходные подблоки раундовых функции F_0, F_1 равны 32 (16) битам. При этом, длины раундовых ключей $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$ необязательно должены быт равны 32 (16) битам.

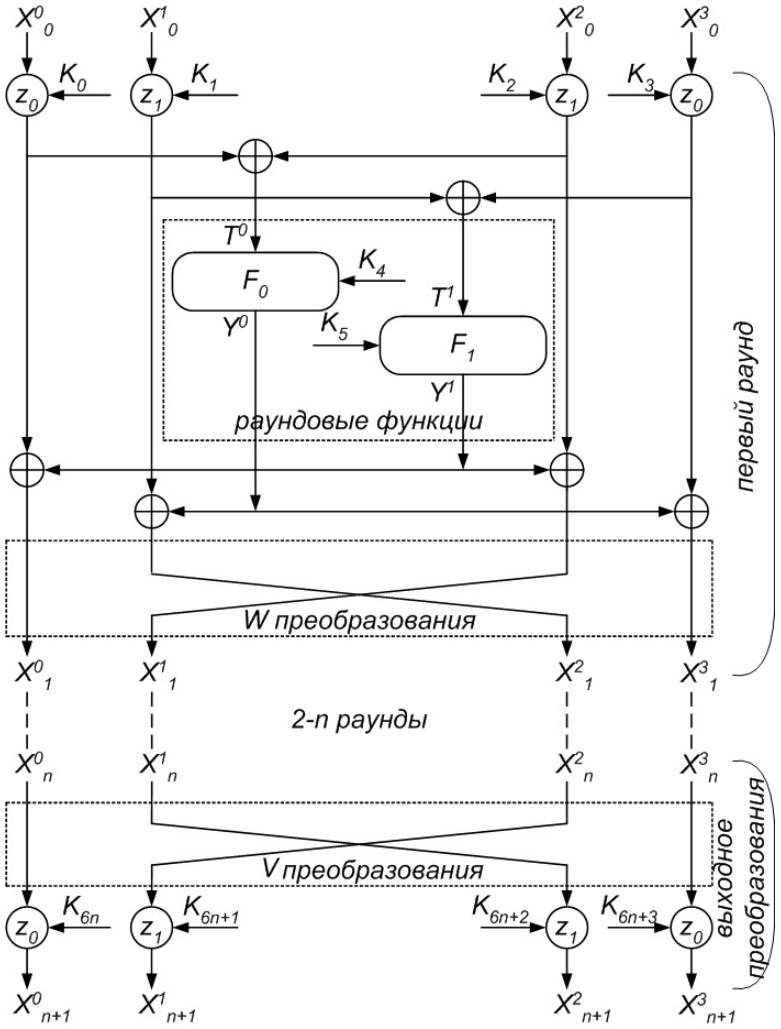


Рис. 3. Схема сети IDEA4–2

В качестве операций z_0, z_1 можно выбрать операции $\otimes$ (mul), $\boxplus$ (add) и $\oplus$ (xor). Здесь $\otimes$–операция умножения 32 (16) битных подблоков по модулю $2^{32}+1$ ($2^{16}+1$), $\boxplus$–операция сложения 32 (16) битных подблоков по модулю 2^{32} (2^{16}) и $\oplus$–операция сложения 32 (16) битных подблоков по XOR.

В *n*–раундовой сети IDEA4–2 в каждом раунде применены шесть и в выходном преобразовании четыре раундовых ключей, т.е. число всех раундовых ключей равно $6n+4$. При зашифровании на рис.3 вместо K_i используются раундовые ключи зашифрования K_i^c, а в расшифровании раундовые ключи расшифрования K_i^d.

Раундовые ключи расшифрования первого раунда связаны к раундовым ключам зашифрования по формуле (1), раундовые ключи выходного преобразования связаны к раундовым ключам зашифрования по формуле (2), раундовые ключи расшифрования второго, третего и *n*–раунда связаны к ключам зашифрования по формуле (3).

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d) = ((K_{6n}^c)^{z_0}, (K_{6n+1}^c)^{z_1}, (K_{6n+2}^c)^{z_1}, (K_{6n+3}^c)^{z_0}, K_{6(n-1)+4}^c, K_{6(n-1)+5}^c) \quad (1)$$

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = ((K_0^c)^{z_0}, (K_1^c)^{z_1}, (K_2^c)^{z_1}, (K_3^c)^{z_0}) \quad (2)$$

$$(K^d_{6(i-1)}, K^d_{6(i-1)+1}, K^d_{6(i-1)+2}, K^d_{6(i-1)+3}, K^d_{6(i-1)+4}, K^d_{6(i-1)+5}) = ((K^c_{6(n-i+1)})^{z_0}, (K^c_{6(n-i+1)+2})^{z_1}, (K^c_{6(n-i+1)+1})^{z_1}, (K^c_{6(n-i+1)+3})^{z_0}, K^c_{6(n-i)+4}, K^c_{6(n-i)+5}), i = \overline{2...n}. \quad (3)$$

Если в качестве операции z_0, z_1 применена mul, то $K = K^{-1}$, если применена add, то $K = -K$ и если применена xor, то $K = K$. Здесь K^{-1}– мультипликативная инверсия числа K, $-K$–аддитивная инверсия числа K. Для 32 битных чисел $K \otimes K^{-1} = 1 \bmod(2^{32}+1)$, для 16 битных чисел $K \otimes K^{-1} = 1 \bmod(2^{16}+1)$ и $-K \boxplus K = 0$, $K \oplus K = 0$.

Для сети IDEA4–2 имеет место следующая теорема:

Теорема 2. В сети IDEA4–2 при вычислении раундовые ключи расшифрования по формуле (1)–(3), зашифровании и расшифровании основано не едином алгоритме.

На основе сети IDEA4–2 разработана сеть IDEA4–1, в которой раундовая функция состоит из двух входных и выходных подблоков, применен один раундовый ключ в раундовой функции, сети RFWKIDEA4–2, RFWKIDEA4–1, в которых раундовые функции сети IDEA4–2 и IDEA4–1 применены без раундовых ключей.

Таким же образом, созданы состоящие из восьми, шестнадцати тридцати и 2m подблоков. В общем случае сети можно привести в виде IDEAX–Y, RFWKIDEAX–Y, здесь X–число подблоков, Y–число раундовых функций. В сети вида IDEAX–Y число раундовых ключей равно (X+Y)n+X, а в сети вида RFWKIDEAX–Y равно Xn+X. Например, сеть IDEA8–4 состоит из восьми подблоков и четырех раундовых функций, каждая раундовая функция имеет один входной и выходной подблок, сеть RFWKIDEA32–2 состоит из тридцати двух подблоков и двух раундовых функций, число входных и выходных подблоков в каждой раундовой функции равно восьми. Число входных и выходных подблоков раундовых функции вычисляется по R=(X/Y)/2.

В сетях вида IDEAX–Y, RFWKIDEAX–Y (X>4) число операций равно X/2. В качестве операций выбраны ⊗– умножение 32 (16, 8) битных блоков по модулю 2^{32}+1 (2^{16}+1, 2^8+1), ⊞–сложение 32 (16, 8) битных блоков по модулю 2^{32} (2^{16}, 2^8) и ⊕–сложение 32 (16, 8) битных блоков по XOR.

В третей главе диссертации **«Сети Лай–Месси вида PESX–Y, RFWKPESX–Y, разработанные на основе структуры алгоритма шифрования PES и схем Лай–Месси»** приведены сети Лай–Месси вида PESX–Y, RFWKPESX–Y, созданные с использованием структуры алгоритма шифрования PES и схемы Лай–Месси. Основным преимуществом сетей является то, что при шифровании и дешифровании используется один и тот же алгоритм и в качестве раундовой функции сети можно использовать любые преобразования.

Сеть PES4–2 приведена на рис.4., длина подблоков X^0, X^1, X^2, X^4, раундовые ключи $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i = \overline{1...n+1}$, входные и выходные подблоки раундовых функции F_0, F_1 равны 32 (16) битам. При

этом длина раундовых ключей $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$ необязательно должна быть равна 32 (16) битам.

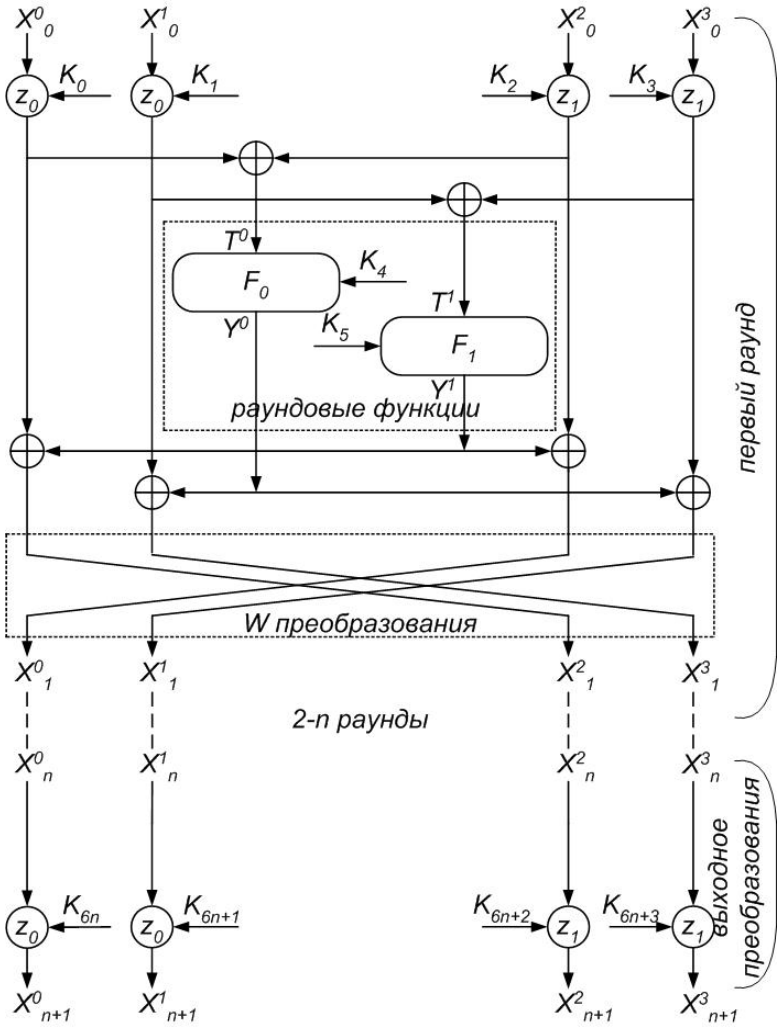


Рис. 4. Схема сети PES4–2

В *n*–раундовой сети PES4–2 в каждом раунде применены шесть и в выходном преобразовании четыре раундовых ключей, т.е. число всех раундовых ключей равно 6*n*+4. Раундовые ключи расшифрования выходного преобразования связаны к раундовым ключам зашифрования по формуле (4), раундовые ключи расшифрования первого, второго и *n*–раунда связаны к ключам зашифрования по формуле (5).

$$(K^d_{6n}, K^d_{6n+1}, K^d_{6n+2}, K^d_{6n+3}) = ((K^c_0)^{z_0}, (K^c_1)^{z_0}, (K^c_2)^{z_1}, (K^c_3)^{z_1}) \quad (4)$$

$$(K^d_{6(i-1)}, K^d_{6(i-1)+1}, K^d_{6(i-1)+2}, K^d_{6(i-1)+3}, K^d_{6(i-1)+4}, K^d_{6(i-1)+5}) = ((K^c_{6(n-i+1)})^{z_0}, (K^c_{6(n-i+1)+1})^{z_0}, (K^c_{6(n-i+1)+2})^{z_1}, (K^c_{6(n-i+1)+3})^{z_1}, K^c_{6(n-i)+4}, K^c_{6(n-i)+5}), i=\overline{1...n}. \quad (5)$$

Для сети PES4–2 имеет место следующая теорема:

Теорема 2. В сети PES4–2 при вычислении раундовые ключи расшифрования по формуле (4), (5), зашифровании и расшифровании основано не едином алгоритме.

Таким же образом, разработаны сети состоящих из четырех, восьми, шестнадцати, тридцати двух и 2m подблоков. В общее случаях сети можно

привести в виде PESX–Y, RFWKPESX–Y. В сети вида PESX–Y число раундовых ключей равно (X+Y)n+X, а в сети вида RFWKPESX–Y равно Xn+X. Например, сеть PES16–4 состоит из щестнадцати подблоков и четырех раундовых функций, каждая раундовая функция имеет две входной и выходной подблок.

В сетях вида PESX–Y, RFWKPESX–Y (X>4) число операций равно двум. В качестве операций выбраны ⊗–умножение 32 (16, 8) битных блоков по модулю, ⊞–сложение 32 (16, 8) битных блоков по модулю 2^{32} (2^{16}, 2^8) и ⊕–сложение 32 (16, 8) битных блоков по XOR.

В четвертой главе диссертации «**Разработанные алгоритмы шифрования, в результате применения раундовой функции алгоритма шифрования AES в качестве раундовых функций сетей Лай–Месси**» приведены алгоритмы шифрования, где раундовые функции алгоритма шифрования AES использованы в качестве раундовых функции сетей Лай–Месси, оценена скорость и стойкость.

Схемы алгоритмов шифрования AES–IDEA8–1 и AES–PES8–1 приведены на рис. 5 и 6. Длина подблоков X^0, X^1, ..., X^7, раундовых ключей $K_{9(i-1)}$, $K_{9(i-1)+1}$, ..., $K_{9(i-1)+7}$, $i=\overline{1...n+1}$, K_{9n+8}, K_{9n+9}, ..., K_{9n+23} равна 32 битам. Длина раундового ключа $K_{9(i-1)+8}$, $i=\overline{1...n}$ равна 128 битам и данный ключ выбран в качестве массива ключа преобразования AddRoundKey(). В алгоритмах шифрования применены преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() алгоритма шифрования AES.

В раундовых функциях алгоритма шифрования 32 битные подблоки T^0, T^1, ..., T^3 разбиваются на 8 битные подблоки, т.е., $t_i = sb_{i \bmod 4}(T^{idiv4})$, $i=\overline{0...15}$. Здесь, *div*–целая часть деления, *mod*–остаток от деления, $sb_0(X)=x_0x_1...x_7$, $sb_1(X)=x_8x_9...x_{15}$, $sb_2(X)=x_{16}x_{17}...x_{23}$, $sb_3(X)=x_{24}x_{25}...x_{31}$ и $X=x_0x_1...x_{31}$. 8 битные подблоки t_0, t_1, ... t_{15} записываются в массиве State. В преобразовании AddRoundKey() 128 битный раундовый ключ $K_{9(i-1)+8}$ разбивается на 32 битные раундовые ключи $K^0_{9(i-1)+8}$, $K^1_{9(i-1)+8}$, $K^2_{9(i-1)+8}$, $K^3_{9(i-1)+8}$. 32 битные раундовые ключи $K^0_{9(i-1)+8}$, $K^1_{9(i-1)+8}$, $K^2_{9(i-1)+8}$, $K^3_{9(i-1)+8}$ разбиваются на 8 битные ключи k_0, k_1, ..., k_{15}, т.е., $k_i = sb_{i \bmod 4}(K^{idiv4}_{9(i-1)+8})$. После чего выполняется преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(). После преобразования AddRoundKey() получатся 8 битные подблоки p'_0, p'_1, ..., p'_{15}. Полученные 8 битные подблоки p'_0, p'_1, ..., p'_{15} записываются в 32 битный подблок Y^0, Y^1, …, Y^3 следующим образом $Y^j = p'_{4j} \| p'_{4j+1} \| p'_{4j+2} \| p'_{4j+3}$, $j=\overline{0...3}$.

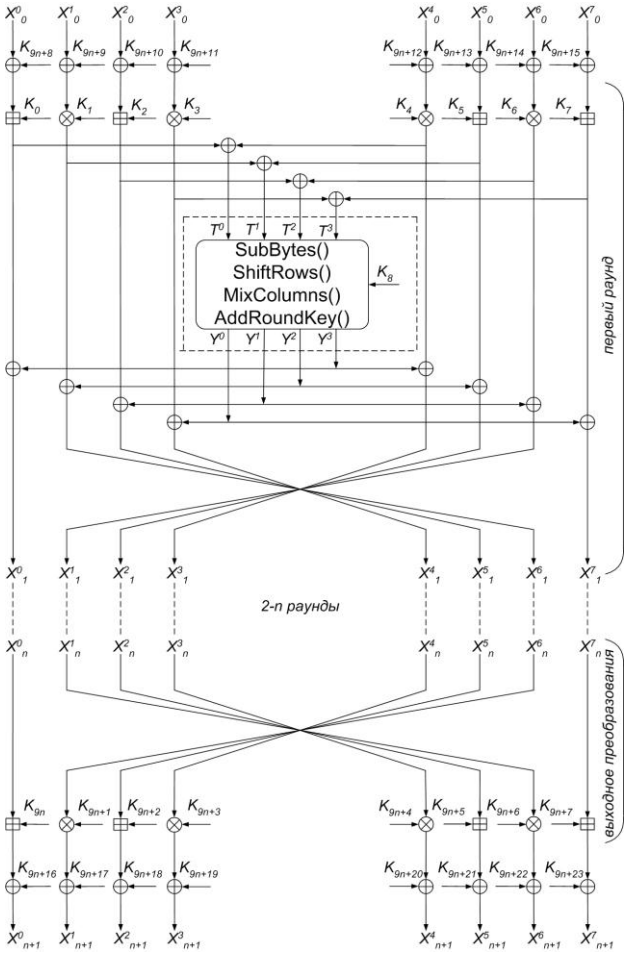


Рис.5. Схема алгоритма шифрования AES–IDEA8–1.

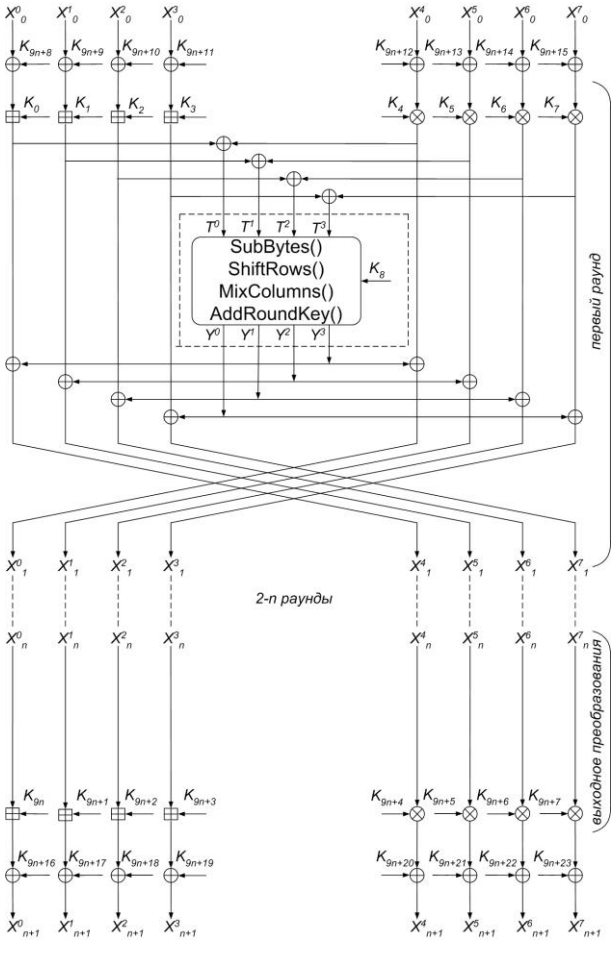


Рис.6. Схема алгоритма шифрования AES–PES8–1.

В *n*–раундовой алгоритмов шифрования AES–IDEA8–1 и AES–PES8–1 в каждом раунде восемь 32 битный, один 128 битный и в выходном преобразовании восем 32 битный раундовые ключи применена. Кроме этого, до первого раунда и после выходного преобразования применена восем 32 битный ключи. Если 128 битный ключ принимается в качестве четырех 32 битных ключи, то число всех 32 битных ключей равно $12n+24$.

Для формирования раундовых ключей шифрования алгоритмов шифрования как у алгоритма AES используется массив Rcon: Rcon=[0x00000001, 0x00000002, 0x00000004, 0x00000008, 0x00000010, 0x00000020, 0x00000040, 0x00000080, 0x00000100, 0x00000200, 0x00000400, 0x00000800, 0x00001000, 0x00002000, 0x00004000, 0x00008000, 0x00010000, 0x00020000, 0x00040000, 0x00080000, 0x00100000, 0x00200000, 0x00400000, 0x00800000, 0x01000000, 0x02000000, 0x04000000, 0x08000000, 0x10000000, 0x20000000, 0x40000000, 0x80000000], т.е состоит из тридцати двух 32 битных значений.

Ключ алгоритма шифрования K длиной l ($256 \le l \le 1024$) разбивается на 32 битные ключи $K_0^{c'}$, $K_1^{c'}$, ..., $K_{Lenght-1}^{c'}$, $Lenght = l/32$. Здесь $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^{c'} = \{k_0, k_1, ..., k_{31}\}$, $K_1^{c'} = \{k_{32}, k_{33}, ..., k_{63}\}$, ..., $K_{Lenght-1}^{c'} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ и $K = K_0^{c'} \| K_1^{c'} \| ... \| K_{Lenght-1}^{c'}$. После чего вычисляется $K_L = K_0^{c'} \oplus K_1^{c'} \oplus ... \oplus K_{Lenght-1}^{c'}$. Если

$K_L = 0$, то в качестве K_L выбирается значение 0xC5C31537, т.е. $K_L = 0xC5C31537$. Раундовые ключи $K_i^{c'}$, $i = \overline{Lenght...12n+23}$ таким образом вычисляется, если $i \bmod 3 = 1$ выполняется $K_i^{c'} = SubBytes32(K_{i-Lenght+1}^{c'}) \oplus SubBytes32(RotWord32(K_{i-Lenght}^{c'})) \oplus Rcon[i \bmod 32] \oplus K_L$, иначе $K_i^{c'} = SubBytes32(K_{i-Lenght}^{c'}) \oplus SubBytes32(K_{i-Lenght+1}^{c'}) \oplus K_L$. После каждой генерации раундовых ключей значение K_L циклический сдвигается налево на 1 бит. Здесь *Rotword32()*–преобразование циклические сдвига 32 битного блока налево на один бит, *SubBytes32()*–преобразования подстановка 32 битного блока в S–блоках, т.е. $SubBytes32(X) = S(sb_0(X)) \| S(sb_1(X)) \| S(sb_2(X)) \| S(sb_3(X))$.

В алгоритме шифрования AES–IDEA8–1 раундовые ключи расшифрования первого раунда связаны с раундовым ключам зашифрования по (6). Раундовые ключи расшифрования выходного преобразования связаны с раундовым ключам зашифрования по (7). Раундовые ключи расшифрования второго, третего и *n*–раунда связаны с раундовым ключам зашифрования по (8):

$$(K_0^{d'}, K_1^{d'}, K_2^{d'}, K_3^{d'}, K_4^{d'}, K_5^{d'}, K_6^{d'}, K_7^{d'}, K_8^{d'}, K_9^{d'}, K_{10}^{d'}, K_{11}^{d'}) = (-K_{12n}^{c'}, (K_{12n+1}^{c'})^{-1}, -K_{12n+2}^{c'}, (K_{12n+3}^{c'})^{-1}, (K_{12n+4}^{c'})^{-1}, -K_{12n+5}^{c'}, (K_{12n+6}^{c'})^{-1}, -K_{12n+7}^{c'}, K_{12(n-1)+8}^{c'}, K_{12(n-1)+9}^{c'}, K_{12(n-1)+10}^{c'}, K_{12(n-1)+11}^{c'}). \quad (6)$$

$$(K_{12n}^{d'}, K_{12n+1}^{d'}, K_{12n+2}^{d'}, K_{12n+3}^{d'}, K_{12n+4}^{d'}, K_{12n+5}^{d'}, K_{12n+6}^{d'}, K_{12n+7}^{d'}) = (-K_0^{c'}, (K_1^{c'})^{-1}, -K_2^{c'}, (K_3^{c'})^{-1}, (K_4^{c'})^{-1}, -K_5^{c'}, (K_6^{c'})^{-1}, -K_7^{c'}). \quad (7)$$

$$(K_{12(i-1)}^{d'}, K_{12(i-1)+1}^{d'}, K_{12(i-1)+2}^{d'}, K_{12(i-1)+3}^{d'}, K_{12(i-1)+4}^{d'}, K_{12(i-1)+5}^{d'}, K_{12(i-1)+6}^{d'}, K_{12(i-1)+7}^{d'}, K_{12(i-1)+8}^{d'}, K_{12(i-1)+9}^{d'}, K_{12(i-1)+10}^{d'}, K_{12(i-1)+11}^{d'}) = (-K_{12(n-i+1)}^{c'}, (K_{6(n-i+1)+6}^{c'})^{-1}, -K_{12(n-i+1)+5}^{c'}, (K_{12(n-i+1)+4}^{c'})^{-1}, (K_{12(n-i+1)+3}^{c'})^{-1}, -K_{6(n-i+1)+2}^{c'}, (K_{12(n-i+1)+1}^{c'})^{-1}, -K_{12(n-i+1)+7}^{c'}, K_{12(n-i)+8}^{c'}, K_{12(n-i)+9}^{c'}, K_{12(n-i)+10}^{c'}, K_{12(n-i)+11}^{c'}), i = \overline{2...n}. \quad (8)$$

В алгоритме шифрования AES–PES8–1 раундовые ключи расшифрования выходного преобразования связаны с раундовым ключам зашифрования по (9). Раундовые ключи расшифрования первого, второго и *n*–раунда связаны с раундовым ключам зашифрования по (10):

$$(K_{12n}^{d'}, K_{12n+1}^{d'}, K_{12n+2}^{d'}, K_{12n+3}^{d'}, K_{12n+4}^{d'}, K_{12n+5}^{d'}, K_{12n+6}^{d'}, K_{12n+7}^{d'}) = (-K_0^{c'}, -K_1^{c'}, -K_2^{c'}, -K_3^{c'}, (K_4^{c'})^{-1}, (K_5^{c'})^{-1}, (K_6^{c'})^{-1}, (K_7^{c'})^{-1}). \quad (9)$$

$$(K_{12(i-1)}^{d'}, K_{12(i-1)+1}^{d'}, K_{12(i-1)+2}^{d'}, K_{12(i-1)+3}^{d'}, K_{12(i-1)+4}^{d'}, K_{12(i-1)+5}^{d'}, K_{12(i-1)+6}^{d'}, K_{12(i-1)+7}^{d'}, K_{12(i-1)+8}^{d'}, K_{12(i-1)+9}^{d'}, K_{12(i-1)+10}^{d'}, K_{12(i-1)+11}^{d'}) = (-K_{12(n-i+1)}^{c'}, -K_{12(n-i+1)+1}^{c'}, -K_{12(n-i+1)+2}^{c'}, -K_{12(n-i+1)+3}^{c'}, (K_{12(n-i+1)+4}^{c'})^{-1}, (K_{12(n-i+1)+5}^{c'})^{-1}, (K_{12(n-i+1)+7}^{c'})^{-1}, (K_{12(n-i+1)+7}^{c'})^{-1}, K_{12(n-i)+8}^{c'}, K_{12(n-i)+9}^{c'}, K_{12(n-i)+10}^{c'}, K_{12(n-i)+11}^{c'}), i = \overline{1...n}. \quad (10)$$

Раундовые ключи расшифрования, применной до первого раунда и после выходного преобразования связаны к ключам зашифрования следующим образом: $K_{12n+8+j}^{d'} = K_{12n+16+j}^{c'}$, $K_{12n+16+j}^{d'} = K_{12n+8+j}^{c'}$, $j = \overline{0...7}$.

Раундовые ключи в зашифровании K_i^c связаны к ключам $K_i^{c'}$ следующим образом: $K_{9i+j}^c = K_{12i+j}^{c'}$, $j = \overline{0...7}$, $K_{9i+8}^c = K_{12i+8}^{c'} \| K_{12i+9}^{c'} \| K_{12i+10}^{c'} \| K_{12i+11}^{c'}$, $K_{9n+j}^c = K_{12n+j}^{c'}$, $j = \overline{0...7}$, $K_{9n+8+j}^c = K_{12n+8+j}^{c'}$, $j = \overline{0...15}$. Таким же образом, раундовые ключи расшифрования K_i^d связаны к ключам $K_i^{d'}$ следующим образом:

$K^d_{9i+j} = K^{d'}_{12i+j}$, $j = \overline{0...7}$, $K^d_{9i+8} = K^{d'}_{12i+8} \| K^{d'}_{12i+9} \| K^{d'}_{12i+10} \| K^{d'}_{12i+11}$, $K^d_{9n+j} = K^{d'}_{12n+j}$, $j = \overline{0...7}$, $K^d_{9n+8+j} = K^{d'}_{12n+8+j}$, $j = \overline{0...15}$.

В качестве раундовых функции сетей вида IDEAX–Y, PESX–Y, RFWKIDEAX–Y, RFWKPESX–Y используя преобразования алгоритма шифрования AES разработаны алгоритмы шифрования вида AES–IDEAX–Y, AES–PESX–Y, AES–RFWKIDEAX–Y, AES–RFWKPESX–Y. Если в алгоритмах шифрования вида AES–IDEAX–Y, AES–PESX–Y применены преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() алгоритма шифрования AES, то в алгоритмах шифрования вида AES–RFWKIDEAX–Y, AES–RFWKPESX–Y применены преобразования SubBytes(), ShiftRows(), MixColumns(). У всех алгоритмов шифрования раундовые ключи измеряется от 256 бита до 1024 бита с шагом 128 бит. В алгоитмах шифрования AES–IDEA8–1, AES–PES8–1, AES–RFWKIDEA8–1, AES–RFWKPES8–1, AES–IDEA16–1, AES–PES16–1, AES–RFWKIDEA16–1, AES–RFWKPES16–1, AES–IDEA32–1, AES–PES32–1, AES–RFWKIDEA32–1, AES–RFWKPES32–1 длина блока равно 256 битам, в алгоитмах шифрования AES–IDEA16–2, AES–PES16–2, AES–RFWKIDEA16–2, AES–RFWKPES16–2 длина блока равно 512 битам, в алгоитмах шифрования AES–IDEA32–4, AES–PES32–4, AES–RFWKIDEA32–4, AES–RFWKPES32–4 длина блока равно 1024 битам. в алгоитмах шифрования AES–IDEA16–1, AES–PES16–1, AES–RFWKIDEA16–1, AES–RFWKPES16–1 длина подблоков равно 16 битам, в алгоитмах шифрования AES–IDEA32–1, AES–PES32–1, AES–RFWKIDEA32–1, AES–RFWKPES32–1 длина подблоков равно 8 битам и осталных алгоритмах шифрования длина подблоков равно 32 битам. Скорости алгоритмов шифрования приведена в 3–таблице.

Параметры S–блоков алгоритмов шифрования равны параметрам S–блоков алгоритма шифрования AES, т.е., $\deg(S) = 7$, $NL(S) = 112$, $\lambda_F = 0.125$, $\delta_F = 1/64$, SAC=8, BIC=8. Для алгоритмов шифрования имеет место следующие утверждение:

Утверждение 5. Общий показатель сложности S–блоков алгоритмов шифрования вида AES–IDEAX–Y, AES–PESX–Y, AES–RFWKIDEAX–Y, AES–RFWKPESX–Y S^8_{index}=0,9382, т.е равно общий показателю сложности алгоритма шифрования AES.

К алгоритмам шифрования применен метод линейного криптоанализа. В процессе применения метода линейного криптоанализа взамен операции умножения в поле использованы операции сложения и не учтены операции, примененные до первого раунда. Результаты вычисления показывают, что стойкость всех алгоритмов шифрования равна. Для применения метода линейного криптоанализа к 4–раундовому алгоритму шифрования потребуется $2^{30.6}$ пар открытого текста–шифртекста, 8–раундовому алгоритму шифрования $2^{61.1}$ пар открытого текста–шифртекста и 12–раундовому алгоритму шифрования $2^{91.1}$ пар открытого текста–шифртекста. Для одного раунда потребуется 202 пар открытого текста–шифртекста и уравнение линейной аппроксимации равно 40. Исползовав операций сложения вместо

умножения и не учитывая операций до первого раунда, стойкость алгоритма сравнительно выше.

3–таблица

Скорости алгоритмов шифрования (Мбайт/с)

Алгоритм шифрования	10 раунд	12 раунд	14 раунд
AES	≈12.812	≈10.682	≈9.224
AES–IDEA8–1, AES–PES8–1	≈14.914	≈12.444	≈10.862
AES–RFWKIDEA8–1	≈16.862	≈14.244	≈12.330
AES–RFWKPES8–1	≈16.862	≈14.244	≈12.330
AES–IDEA16–1, AES–PES16–1	≈15.444	≈12.952	≈11.242
AES–RFWKIDEA16–1	≈17.808	≈14.902	≈12.944
AES–RFWKPES16–1	≈17.808	≈14.902	≈12.944
AES–IDEA32–1, AES–PES32–1	≈15.534	≈13.080	≈11.248
AES–RFWKIDEA32–1	≈17.094	≈14.566	≈12.444
AES–RFWKPES32–1	≈17.094	≈14.566	≈12.444
AES–IDEA16–2, AES–PES16–2	≈15.082	≈12.570	≈10.770
AES–RFWKIDEA16–2	≈17.294	≈14.082	≈12.330
AES–RFWKPES16–2	≈17.294	≈14.082	≈12.330
AES–IDEA32–4, AES–PES32–4	≈15.082	≈12.820	≈10.774
AES–RFWKIDEA32–4	≈16.876	≈14.184	≈12.210
AES–RFWKPES32–4	≈16.876	≈14.184	≈12.210

В пятой главе диссертации «**Разработанные алгоритмы шифрования, в результате применения раундовой функции алгоритма шифрования ГОСТ 28147–89 в качестве раундовых функций сетей Лай–Месси**» приведены алгоритмы шифрования, где раундовые функции алгоритма шифрования ГОСТ 28147–89 использованы в качестве раундовых функции сетей Лай–Месси, оценена скорость и стойкость.

Схемы алгоритмов шифрования GOST28147–89–IDEA4–2 и GOST28147–89–PES4–2 приведены на рис. 7 и 8. Длина подблоков X^0, X^1, X^2, X^3, раундовых ключей $K_{6(i-1)}$, $K_{6(i-1)+1}$, $K_{6(i-1)+2}$, $K_{6(i-1)+3}$, $i=\overline{1...n+1}$, $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$, K_{6n+4}, K_{6n+5}, ..., K_{6n+11}, входные и выходные подблоки раундовой функции равны 32 битам.

В раундовых функциях алгоритма шифрования 32 битные подблоки T^0, T^1 суммируются с раундовыми ключами $K_{6(i-1)+4}$, $K_{6(i-1)+5}$, $i=\overline{1...n}$, т.е., $S^0=T^0+K_{6(i-1)+4}$, $S^1=T^1+K_{6(i-1)+5}$. 32 битные подблоки разбиваются на восемь четырех битных подблока $S^0=s_0^0\|s_1^0\|s_2^0\|s_3^0\|s_4^0\|s_5^0\|s_6^0\|s_7^0$, $S^1=s_0^1\|s_1^1\|s_2^1\|s_3^1\|s_4^1\|s_5^1\|s_6^1\|s_7^1$. 4 битные подблоки s_i^0, s_i^1, $i=\overline{0...7}$ преобразуются в S–блоках, т.е., $R^0=S_0(s_0^0)\|S_1(s_1^0)\|S_2(s_2^0)\|S_3(s_3^0)\|S_4(s_4^0)\|S_5(s_5^0)\|S_6(s_6^0)\|S_7(s_7^0)$, $R^1=S_8(s_0^1)\|S_9(s_1^1)\|S_{10}(s_2^1)\|S_{11}(s_3^1)\|S_{12}(s_4^1)\|S_{13}(s_5^1)\|S_{14}(s_6^1)\|S_{15}(s_7^1)$. Полученные 32 битные подблоки R^0, R^1

циклически сдвигаются налево на 11 бит и получаются подблоки Y^0, Y^1: $Y^0 = R^0 <<11$, $Y^1 = R^1 <<11$.

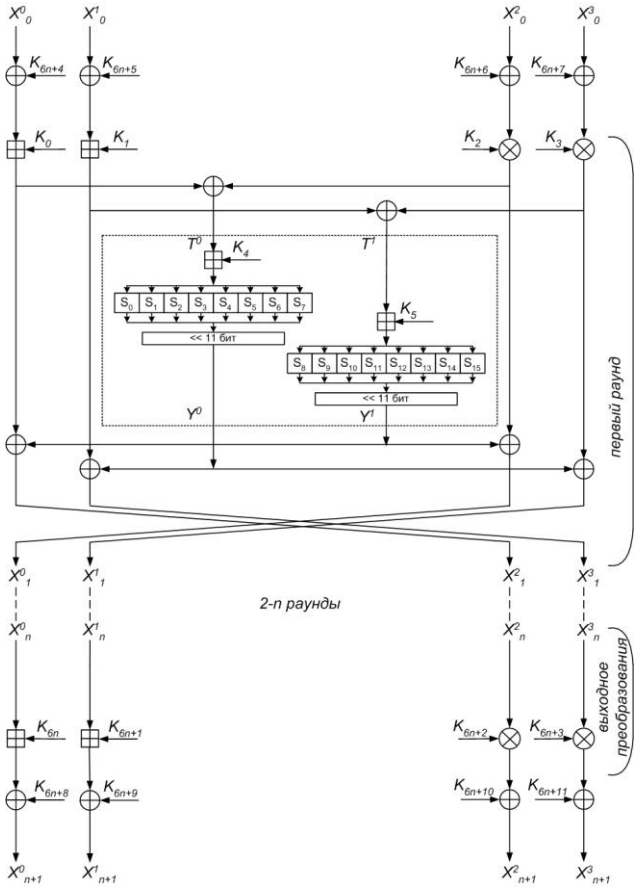


Рис.7. Схема алгоритма шифрования GOST28147–89–IDEA4–2.

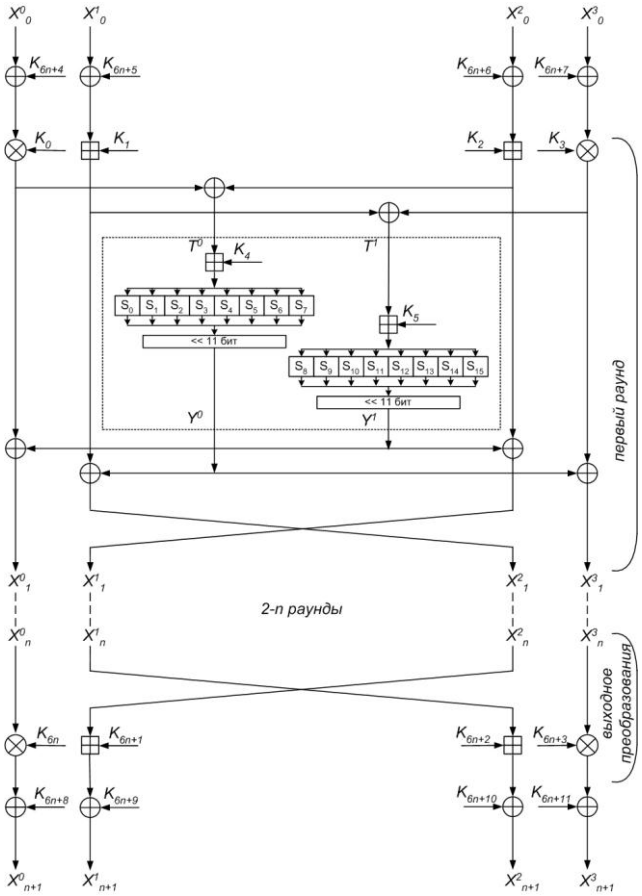


Рис.8. Схема алгоритма шифрования GOST28147–89–PES4–2.

В *n*–раундых алгоритмах шифрования GOST28147–89–IDEA4–2 и GOST28147–89–PES4–2 до первого раунда и после входного преобразования четыре 32 битный ключи, в каждом раунде шесть 32 битный ключи, в выходном преобразовании четыре 32 битный ключи применена, т.е число всех раундовых ключей равно 6*n*+12. В алгоритме шифрования при равенстве чисел раундов 8, 12 и 16 генерируется 32 битные 60, 84 и 108 раундовые ключи.

Ключ алгоритма шифрования *K* длиной *l* ($256 \le l \le 1024$) разбивается на 32 битных ключей K_0^c, K_1^c, ..., $K_{Lenght-1}^c$, $Lenght = l/32$, здесь $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, ..., k_{63}\}$, ..., $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ и $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$. После чего вычисляется $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$. Если $K_L = 0$, то в качестве K_L выбирается значение 0xC5C31537. А раундовые ключи K_i^c, $i = \overline{Lenght...6n+11}$ вычисляется как $K_i^c = SBox0(K_{i-Lenght}^c) \oplus SBox1(RotWord(K_{i-Lenght+1}^c)) \oplus K_L$, после каждого генерации раундовых ключей значений K_L сдвигается налево на 1 бит. Здесь *Rotword()*–преобразования циклического сдвига 32 битного блока налево на 1 бит, *Sbox()*–подстановка в

S–блоке 32 битного блока и $SBox0(A) = S_0(a_0) \| \ S_1(a_1) \| S_2(a_2) \| S_3(a_3) \| S_4(a_4) \| S_5(a_5) \| S_6(a_6) \| S_7(a_7)$, $SBox1(A) = S_8(a_0) \| S_9(a_1) \| S_{10}(a_2) \| \ S_{11}(a_3) \| S_{12}(a_4) \| S_{13}(a_5) \| S_{14}(a_6) \| S_{15}(a_7)$, $A = a_0 \| a_1 \| a_2 \| a_3 \| a_4 \| a_5 \| a_6 \| a_7$, здесь a_i–четырех битные подблоки.

В алгоритме шифрования GOST28147–89–IDEA4–2 раундовые ключи расшифрования первого раундка связаны с раундовым ключа зашифрования по (11). Раундовые ключи расшифрования выходного преобразования связаны с раундовым ключа зашифрования по (12). Раундовые ключи расшифрования второго, третего и *n*–раунда связаны к раундовым ключа зашифрования по (13).

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d) = ((K_{6n}^c)^{-1}, -K_{6n+1}^c, -K_{6n+2}^c, (K_{6n+3}^c)^{-1}, K_{6(n-1)+4}^c, K_{6(n-1)+5}^c) \quad (11)$$

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = ((K_0^c)^{-1}, -K_1^c, -K_2^c, (K_3^c)^{-1}) \quad (12)$$

$$\begin{aligned}&(K_{6(i-1)}^d, K_{6(i-1)+1}^d, K_{6(i-1)+2}^d, K_{6(i-1)+3}^d, K_{6(i-1)+4}^d, K_{6(i-1)+5}^d) = ((K_{6(n-i+1)}^c)^{-1}, -K_{6(n-i+1)+2}^c, \\ &-K_{6(n-i+1)+1}^c, (K_{6(n-i+1)+3}^c)^{-1}, K_{6(n-i)+4}^c, K_{6(n-i)+5}^c), i = \overline{2...n}.\end{aligned} \quad (13)$$

В алгоритме шифрования GOST28147–89–PES4–2 раундовые ключи расшифрования первого, второго и *n*–раунда связаны с раундовым ключам зашифрования по формуле (14). Раундовые ключи расшифрования выходного преобразования связаны с раундовым ключа зашифрования по формуле (15).

$$(K_{6n}^d, K_{6n+1}^d, K_{6n+2}^d, K_{6n+3}^d) = (-K_0^c, -K_1^c, (K_2^c)^{-1}, (K_3^c)^{-1}) \quad (14)$$

$$\begin{aligned}&(K_{6(i-1)}^d, K_{6(i-1)+1}^d, K_{6(i-1)+2}^d, K_{6(i-1)+3}^d, K_{6(i-1)+4}^d, K_{6(i-1)+5}^d) = (-K_{6(n-i+1)}^c, -K_{6(n-i+1)+1}^c, \\ &(K_{6(n-i+1)+2}^c)^{-1}, (K_{6(n-i+1)+3}^c)^{-1}, K_{6(n-i)+4}^c, K_{6(n-i)+5}^c), i = \overline{1...n}.\end{aligned} \quad (15)$$

Раундовые ключи расшифрования, применной до первого раунда и после выходного преобразования связаны с ключам зашифрования следующим образом: $K_{6n+4+j}^d = K_{6n+8+j}^c$, $K_{6n+8+j}^d = K_{6n+4+j}^c$, $j = \overline{0...3}$.

Кроме этого, в качестве раундовых функции сетей вида IDEAX–Y, PESX–Y, RFWKIDEAX–Y, RFWKPESX–Y используя преобразования алгоритма шифрования ГОСТ 28147–89 разработаны алгоритмы шифрования вида GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y. Если в алгоритмах шифрования вида GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y преобразования алгоритма шифрования ГОСТ 28147–89 использовано в полном объёме, то в алгоритмах шифрования GOST28147–89–RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y применена преобразования подстановка в S–блоках и циклический сдвиг налево. У всех алгоритмов шифрования раундовые ключи измеряется от 256 бита до 1024 бита с шагом 128 бит. Длина блока алгоитмов шифрования GOST28147–89–IDEA4–2, GOST28147–

89–RFWKIDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, GOST28147–89–IDEA16–2, GOST28147–89–RFWKIDEA16–2, GOST28147–89–PES16–2, GOST28147–89–RFWKPES16–2 равно 128 битам, длина блока алгоитмов шифрования GOST28147–89–IDEA8–4, GOST28147–89–RFWKIDEA8–4, GOST28147–89–PES8–4, GOST28147–89–RFWKPES8–4 равно 256 битам. Длина подблока алгоритмов шифрования GOST28147–89–IDEA16–2, GOST28147–89–RFWKIDEA16–2, GOST28147–89–PES16–2, GOST28147–89–RFWKPES16–2 равно 8 битам и осталных алгоритмах шифрования длина подблоков равно 32 битам. Скорости алгоритмов шифрования приведена в 4–таблице.

4–таблица

Скорости алгоритмов шифрования (Мбайт/с)

Шифрлаш алгоритмлари	8 раунд	12 раунд	14 раунд
ГОСТ 28147–89 (32 раунд)	≈27.855		
GOST28147–89–IDEA4–2	≈40.029	≈29.069	≈22.123
GOST28147–89–RFWKIDEA4–2	≈40.145	≈30.228	≈22.883
GOST28147–89–PES4–2	≈40.029	≈29.069	≈22.123
GOST28147–89–RFWKPES4–2	≈40.145	≈30.228	≈22.883
GOST28147–89–IDEA8–4	≈40.015	≈29.047	≈22.059
GOST28147–89–RFWKIDEA8–4	≈40.137	≈30.103	≈22.819
GOST28147–89–PES8–4	≈40.015	≈29.047	≈22.059
GOST28147–89–RFWKPES8–4	≈40.137	≈30.103	≈22.819
GOST28147–89–IDEA16–2	≈33.783	≈24.691	≈18.315
GOST28147–89–RFWKIDEA16–2	≈33.846	≈24.813	≈18.867
GOST28147–89–PES16–2	≈33.783	≈24.691	≈18.315
GOST28147–89–RFWKPES16–2	≈33.846	≈24.813	≈18.867

Вычислены параметры S–блоков алгоритмов шифрования и $NL(S)=4$, $\deg(S)=3$, $\lambda_F=8/16$, $\delta_F=6/16$, SAC=2, BIC=4. Для алгоритмов шифрования имеет место следующее утверждение.

Утверждение 6. Общий показатель сложности S–блоков алгоритмов шифрования вида GOST28147–89–IDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–RFWKPESX–Y S^4_{index}=0,8916, т.е выше чем общий показатель сложности алгоритма шифрования ГОСТ 28147–89.

К алгоритмам шифрования примен метод линейного криптоанализи. В процессе применения метода линейного криптоанализа взамены операции умножения в поле использован операции сложения. Не учтены операции, использованные до первого раунда и после выходного преобразования. Результат вычисления приведена в 5–таблице.

5–таблица

Результаты метода линейного криптоанализа

Шифрлаш алгоритмлари	4 раунд	8 раунд	12 раунд
GOST28147–89–IDEA4–2	2^{35}	2^{70}	2^{104}
GOST28147–89–PES4–2	2^{35}	2^{70}	2^{104}
GOST28147–89–RFWKIDEA4–2	2^{27}	$2^{54.5}$	2^{81}
GOST28147–89–RFWKPES4–2	2^{27}	$2^{54.5}$	2^{81}
GOST28147–89–IDEA8–4	2^{83}	–	–
GOST28147–89–PES8–4	2^{83}	–	–
GOST28147–89–RFWKIDEA8–4	2^{75}	–	–
GOST28147–89–RFWKPES8–4	2^{75}	–	–
GOST28147–89–IDEA16–2	2^{51}	2^{102}	–
GOST28147–89–PES16–2	2^{51}	2^{102}	–
GOST28147–89–RFWKIDEA16–2	2^{43}	2^{86}	–
GOST28147–89–RFWKPES16–2	2^{43}	2^{86}	–

Как видно из таблицы, использовав операции сложения вместо умножения, не учитывая операции до первого раунда и после выходного преобразования стойкость алгоритма сравнительно выше.

ЗАКЛЮЧЕНИЯ

В результате исследований, проведенных по докторской диссертации на тему «Теория и практика функциональной сети Лай–Месси, основанной на едином алгоритме», представлены следующие выводы:

1. Разработаны сети Лай–Месси в виде IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y (X–число подблоков, Y–число раундовых функции), состоящие из раундовых функций. В сетях при зашифровании и дешифровании возможно использование один и тот же алгоритма. Доказано что при зашифровании и расшифровании используется один и тот де алгоритм.

2. В разработанных сетях число блоков равно 4, 8, 16, 32 и 2m, а длина подблоков 8, 16 и 32 битам. В качестве раундовых функций сетей в виде IDEAX–Y, RFWKIDEAX–Y, PESX–Y, RFWKPESX–Y берутся преобразования в который входные и выходные подблоки равно 1, 2, 4, 8, 16, 32 и *m* подблоки длиной 8, 16 и 32 бита, при длине подблоков 8, 16 и 32 бита в основе сети дает возможность создать алгоритмы шифрования длиной блоков 8X, 16X и 32X бита.

3. Разработанные на основе конструкции Ниберга стойкие S–блоки размером 4x4, 8x8 служат созданию новых блоков алгоритмов шифрования.

4. В результате применения раундовой функции алгоритма шифрования AES в качестве раундовых функций сетей Лай–Месси разработаны алгоритмы шифрования AES–IDEAX–Y, AES–RFWKIDEAX–Y, AES–PESX–Y, AES–RFWKPESX–Y. Скорость и стойкость алгоритмов

шифрования выше, чем у алгоритма шифрования AES. Количество раундов алгоритмов шифрования равно 10, 12 и 14, длина ключа меняется от 256 до 1024 битов. Позволяет выбрать длину ключа в зависимости от секретности информации и скорости шифрования. Применение алгоритмов приводит к повышению скорости на 16–38 % и повышении стойкости к линейному криптоанализу до 60%.

5. В результате применения раундовой функции алгоритма шифрования ГОСТ 28147–89 в качестве раундовых функции сетей Лай–Месси разработаны алгоритмы шифрования GOST28147–89–IDEAX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKPESX–Y. Количество раундов алгоритмов шифрования равно 8, 12 и 16, длина ключа меняется от 256 до 1024 битов. Позволяет выбрать длину ключа в зависимости от секретности информации и скорости шифрования.

6. Скорость всех 8–раундовых алгоритмов и 12–раундовых алгоритмов шифрования GOST28147–89–IDEA4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, GOST28147–89–IDEA8–4, GOST28147–89–RFWKIDEA8–4, GOST28147–89–PES8–4, GOST28147–89–RFWKPES8–4 выше, чем скорость алгоритма шифрования ГОСТ 28147–89. Стойкость алгоритмов шифрования выше, чем у алгоритма шифрования ГОСТ 28147–89. Применение алгоритмов служит повышению стойкости к линейному криптоанализу до 60%, а в некоторых случаях и повышении скорости.

SCIENTIFIC COUNCIL DSc.27.06.2017.FM.01.02 AWARDING SCIENTIFIC DEGREES AT NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN

TUYCHIEV GULOM NUMONOVICH

THEORY AND PRACTICE OF THE FUNCTIONAL LAI–MASSEY NETWORK, BASED ON A COMMON ALGORITHM

05.01.05–Methods and systems of information protection. Information security

ABSTRACT OF DOCTORAL (DSc) DISSERTATION OF PHYSICO–MATHEMATICAL SCIENCES

Tashkent–2017

The subject of doctoral dissertation is registered on B2017.1.DSc/FM3 at the Supreme Attestation Commission of the Cabinet of Ministers of the Republic of Uzbekistan

Dissertation is carried out at the National university of Uzbekistan.

Abstract of dissertation in three languages (uzbek, russian, english (resume)) in placed on web–page scientific council (www.nuu.uz) and educational informational networks «ZIYONET» (www.ziyonet.uz)

Scientific consultant:	**Aripov Mirsaid Mirsidikovich** doctor of physics–mathematics sciences, professor
Official opponents:	**Karimov Madjid Malikovich** doctor of technical sciences, professor
	Kasimov Nadimullo Khabibullaevich doctor of physics–mathematics sciences, professor
	Uteuliev Nietbai Uteulievich doctor of physics–mathematics sciences, professor
Leading organization:	**SUE «UNICON.UZ»**

Defence will take place «__» _____ 2017 y. at 10^{00} at the meeting of scientific council number DSc.27.06.2017.FM.01.02 at National university of Uzbekistan (Address: 100174, Tashkent, VUZ Gorodok, Universitet–4 str. Ph.: (99871) 246–02–24; fax: (99871) 246–53–21; e–mail: info@nuu.uz)

Doctoral dissertation can be reviewed in Information–resources centre at National university of Uzbekistan (registration number _____). Address: 100174, Tashkent, VUZ Gorodok, Universitet–4 str. Ph.: (99871) 246–02–24; fax: (99871) 246–53–21; e–mail:info@nuu.uz

Abstract of dissertation sent out on «___» _____ 2017 year.
(mailing report № _____ on «___» _____ 2017 y.).

A.R.Marakhimov
Chairman of scientific council on award
of scientific degree D.T.S.

Z.R.Raxmonov
Scientific secretary of scientific council on award of
scientific degree D.Ph–M.S.

R.D.Aloev
Chairman of scientific seminar under scientific council
on award of scientific degree, D.Ph–M.S.

ABSTRACT (introduction)
of the doctoral (DSc) dissertation of physico–mathematical sciences

The aim of the research is development Lai–Massey network, encryption algorithms based on this network and generation resistance S–boxes.

The objectives of the research are the Lai–Massey networks, Nyberg construction.

Scientific novelty of the research is as follows**:**

created Lai–Massey networks form IDEAX–Y, RFWKIDEAX–Y using the structure of encryption algorithm IDEA and Lai–Massey scheme;

created Lai–Massey networks form PESX–Y, RFWKPESX–Y using the structure of encryption algorithm PES and Lai–Massey scheme;

developed encryption algorithms form AES–IDEAX–Y, AES–RFWKIDEAX–Y, AES–PESX–Y, AES–RFWKPESX–Y as a result of applying the round function of the encryption algorithm AES as the round functions of Lai–Massey networks;

developed encryption algorithms form GOST28147–89–IDEAX–Y, GOST28147–89–RFWKIDEAX–Y, GOST28147–89–PESX–Y, GOST28147–89–RFWKPESX–Y as a result of applying the round function of encryption algorithms GOST 28147–89 as round functions of Lai–Massey networks;

on the basis of Nyberg construction developed resistance S–box size of 8x8, 4x4.

Implementation of the research results. On the base of Lai–Massey network, based on a single algorithm:

encryption algorithm AES–IDEA32–4 created using round transformations of encryption algorithm AES, implemented in the software «Himfayl» in SUE «UNICON.UZ» (certificate of the Ministry of Information Technologies and Communications of May 29, 2017 No. 33–8 / 3256). Availability capabilities choice key length and number of rounds in the encryption algorithm AES–IDEA32–4, and application of encryption algorithms in file protection arbitrary format led to an increase in encryption speed by 17%.

encryption algorithm GOST28147–89–IDEA16–2 created using round transformations of encryption algorithm AES, implemented in the software «Himfayl» in SUE «UNICON.UZ» (certificate of the Ministry of Information Technologies and Communications of May 29, 2017 No. 33–8 / 3256). Availability capabilities choice key length and number of rounds in the encryption algorithm GOST28147–89–IDEA16–2, and application of encryption algorithms in file protection arbitrary format led to an increase in encryption speed by 21%.

The results of the dissertation encryption algorithms AES–PES16–1, AES–RFWKPES16–1, AES–RFWKPES32–1, AES–RFWKIDEA32–1 are used in foreign scientific works (International Journal of Network Security, vol.19, No.6, pp.899–903, Nov. 2017; International Journal of Network Security, vol.19, No.6, pp.984–994, Nov. 2017; International Journal of Network Security, vol.19, No.3, pp.413–420, May 2017; Displays, vol.49, pp.116–123, Sep. 2017). The application of scientific results allows for the construction of further characterization of H–

vectorial functions, hiding information in binary images, when protecting large images, cryptographically model for efficient multiple keyword–based search over encrypted data by secure index.

Publication of the results. On the topic of the dissertation published only 50 scientific papers, in t.ch. 21 articles (13 in the republican and 8 in foreign journals) published in scientific publications, recommended by the Higher Attestation Commission of the Republic of Uzbekistan for the main scientific results of doctoral dissertations. 6 certificates on registration of software for computers have been received.

The outline of the thesis. The thesis consists of an introduction, five chapters, conclusion, a list of used literature and applications. The volume of the thesis is 198 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (I часть; I part)

1. Арипов М.М., Туйчиев Ғ.Н. Иккита раунд функциядан иборат IDEA4–2 тармоғи // Ахборот коммуникациялари: Тармоқлар–Технологиялар–Ечимлар. –Тошкент. 2012. №4 (24). 55–59 б. (05.00.00, №2).
2. Туйчиев Ғ.Н. Тўртта раунд функциядан иборат IDEA8–4 тармоғи // Ахборот коммуникациялари: Тармоқлар–Технологиялар–Ечимлар. –Тошкент. 2013. №2 (26). 55–59 б. (05.00.00, №2).
3. Туйчиев Ғ.Н. ГОСТ 28147–89 блокли шифрлаш алгоритми раунд функциясидан фойдаланилган ҳолда IDEA4–2 тармоғига асосланган блокли шифрлаш алгоритми яратиш // Ахборот коммуникациялари: Тармоқлар–Технологиялар–Ечимлар. –Тошкент. 2014. №4 (32). 49–54 б. (05.00.00, №2).
4. Туйчиев Ғ.Н. IDEA32–16 тармоғи асосида яратилган IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1 тармоқлари ҳақида // Ахборот коммуникациялари: Тармоқлар–Технологиялар–Ечимлар. –Тошкент. 2014. №2(30). 45–50 б. (05.00.00, №2).
5. Туйчиев Ғ.Н. AES–RFWKIDEA16–1 блокли шифрлаш алгоритми // Ахбороткоммуникациялар: Тармоқлар–Технологиялар–Ечимлар. –Тошкент. 2015. №2 (34). 48–54 б. (05.00.00, №2).
6. Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанные на основе сети IDEA8–4 // Узбекский математический журнал. –Ташкент. 2014. №3. –с. 104–118 (01.00.00, №6).
7. Туйчиев Ғ.Н. Саккизта раунд функциядан иборат IDEA16–8 тармоғи // ТошДТУ хабарлари. –Тошкент. 2014. №1. 183–187 б. (05.00.00, №16).
8. Туйчиев Ғ.Н. Ўн олтита раунд функциядан иборат IDEA32–16 тармоғи // ЎзМУ хабарлари. –Тошкент. 2013. №4/1. 57–61 б. (01.00.00, №8)
9. Туйчиев Ғ.Н. Туйчиев Ғ.Н. AES шифрлаш алгоритми акслантиришларидан фойдаланилган ҳолда IDEA32–1 тармоғига асосланган блокли шифрлаш алгоритми яратиш // ЎзМУ хабарлари. –Тошкент. 2015. №2/1. 136–142 б. (01.00.00, №8).
10. Туйчиев Ғ.Н. Иккита раунд функциядан иборат PES4–2 тармоғи // Информатика ва энергетика муаммолари Ўзбекистон журнали, –Тошкент. 2013. №5–6. 107–111 б. (05.00.00, №5).
11. Туйчиев Ғ.Н. PES4–2 тармоғи асосида яратилган PES4–1, RFWKPES4–2, PES4–1 тармоқлари ҳақида // Информатика ва энергетика муаммолари Ўзбекистон журнали. –Тошкент. 2015. №1–2. 100–105 б. (05.00.00, №5).
12. Туйчиев Г.Н. Применение булевых функции в оценки стойкости S–блоков // Доклады Академии наук Республики Узбекистан. –Ташкент. 2010. №1, –с.24–28 (01.00.00, №7).

13. Tuychiev G. Creating a encryption algorithm based on network PES4–2 with the use the round function of the GOST 28147–89 // TUIT Bulleten. – Tashkent. 2015. №2(34). –pp.132–136 (05.00.00, №10).

14. Tuychiev G. Creating a encryption algorithm based on network RFWKIDEA4–2 with the use the round function of the GOST 28147–89 // International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science (ICDAVIM–2015), //printed in International Journal of Advanced Technology in Engineering and Science. 2015. vol. 3. №1. –pp.427–432. (№5), GIF=0.569.

15. Tuychiev G. New encryption algorithm based on network IDEA8–1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science. 2015. Volume 3. Issue 1. –pp.1–6. (№22), ISRA=1.925.

16. Tuychiev G. New encryption algorithm based on network RFWKIDEA8–1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security. 2015. Vol. 3. №. 2. –pp.43–47. (№5), GIF=0.675.

17. Tuychiev G. New encryption algorithm based on network RFWKPES8–1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security. 2014. vol.3. №6. –pp.31–34. (№5), GIF=0.564.

18. Tuychiev G. New encryption algorithm based on network IDEA16–1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Information Technology. 2015. Vol. 3. Issue 1. –pp.6–12. (№22), ISRA=1.801.

19. Tuychiev G. The encryption algorithms AES–PES16–1 and AES–RFWKPES16–1 based on networks PES16–1 and RFWKPES16–1 // International Journal of Electronics and Information Engineering. 2015, Vol.3. No.2. –pp.53–66. (№43), UIF=28.4587.

20. Aripov M., Tuychiev G. The Encryption Algorithm AES–RFWKPES32–4 // International Journal of Electronics and Information Engineering. 2016. Vol.5. No.1. –pp.20–29. (№43), UIF=28.4587.

21. Tuychiev G. The block encryption algorithms GOST28147–89–PES16–2 and GOST28147–89–RFWKPES16–2 // International Journal of Electronics and Information Engineering. 2017, Vol.6. No.1. –pp.1–11. (№43), UIF=28.4587.

II бўлим (II часть; II part)

22. Туйчиев Ғ.Н. RFWKIDEA4–2, IDEA4–1 ва RFWKIDEA4–1 тармоқлари // Тошкент шаҳридаги Турин политехника университети ахборотномаси. –Тошкент. 2013. №3. 71–77 б.

23. Туйчиев Ғ.Н. IDEA16–8 тармоғи асосида яратилган IDEA16–4, IDEA16–2, IDEA16–1 тармоқлари ҳақида // «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал этиш йўллари» республика семинари маърузалар ва тезислар тўплами. –Тошкент. 2014 й.

24. Tuychiev G.N. To the networks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 and RFWKIDEA32–1, based on the network IDEA32–16 // International Journal on Cryptography and Information Security (IJCIS). 2015. Vol. 5. No. 1. –pp. 9–20.

25. Туйчиев Г.Н. О сети IDEA2m–m, состоящей из m раундовых функций и её модификации // II Международная научно–практическая Интернет–конференция «Информационная и экономическая безопасность» (INFECO–2015) // опубликован в журнале Системы обработки информации. – Харков. 2015. – Вып. 7(132). –с.136–147.

26. Арипов М.М., Туйчиев Ғ.Н. Тўртта раунд функциядан иборат PES8–4 тармоғи // «Амалий математика ва информацион технологияларнинг долзарб муаммолари–Ал–Хоразмий 2012» Халқаро илмий анжуман материаллари, тўплам № II. –Тошкент. 2012, 16–19 б.

27. Туйчиев Ғ.Н. PES8–4 тармоги асосида яратилган PES8–2 ва PES8–1 тармоклари хакида // «Амалий математика ва информацион технологияларнинг долзарб муаммолари–Ал–Хоразмий 2014» Халқаро анжуман маърузалар тўплами, тўплам № 2. –Самарқанд. 2014. 28–32 б.

28. Туйчиев Ғ.Н. PES8–4 тармоги асосида яратилган RFWKPES8–4, RFWKPES8–2, RFWKPES8–1 тармоклари хакида // «Амалий математика ва информацион технологияларнинг долзарб муаммолари–Ал–Хоразмий 2014» Халқаро анжуман маърузалар тўплами, тўплам № 2. –Самарқанд. 2014. 32–36 б.

29. Туйчиев Ғ.Н. PES32–16 тармоғи асосида яратилган RFWKPES32–16, RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 ва RFWKPES32–1 тармоқлари ҳақида // «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал этиш йўллари» республика семинари маърузалар ва тезислар тўплами. –Тошкент. 2014.

30. Туйчиев Г.Н. О сети PES2m–m, состоящей из m раундовых функций и её модификации // Безопасность информации. –Киев. 2015. Том 21. №1. –с. 52–63.

31. Арипов М.М., Туйчиев Г.Н. О генерации S блоков размером 8x8 // «Информационная безопасность в свете Стратегии Казахстан–2050»: Сборник трудов I Международной научно–практической конференции (12 сентября 2013 г., Астана). – Астана. 2013. –с.116–125.

32. Туйчиев Г.Н. Генерация стойких булевых функций на основе конструкции Ниберг и ее применение // «Информационная безопасность в свете Стратегии Казахстан–2050»: Сборник трудов II Международной научно–практической конференции (15–17 октября 2014 г., Астана). – Астана. 2014. –с.205–214.

33. Бахтиёров У.Б., Туйчиев Ғ.Н. О генерации стойких S–блоков размером 4x4 и булевы функции на основе конструкции Нюберга // Материалы научно–технической конференции «Прикладная математика и информационная безопасность», –Ташкент. 2014. 28–30 апреля. –с.317–324.

34. Tuychiev G. The Encryption Algorithms GOST–IDEA16–2 and GOST–RFWKIDEA16–2 // Global journal of Computer science and technology: E Network, Web & security. vol 16. Issue 1. 2015. –pp.30–38.

35. Tuychiev G. Creating a encryption algorithm based on network RFWKPES4–2 with the use the round function of the GOST 28147–89 // International Journal of Multidisciplinary in Cryptology and Information Security. 2015. vol.4. №2. –pp.14–17.

36. Tuychiev G. The encryption algorithm AES–RFWKIDEA32–1 based on network RFWKIDEA32–1 // Global journal of Computer science and technology: E Network, Web & security. 2016. vol 15. Issue 4. –pp.33–41.

37. Tuychiev G. The encryption algorithms GOST28147–89–IDEA8–4 and GOST28147–89–RFWKIDEA8–4 // Global journal of Computer science and technology: C Software & Data Engineering. 2016. vol 16. Issue 5. –pp.29–36.

38. Туйчиев Г.Н. О сетях RFWKIDEA16–8, RFWKIDEA16–4, RFWKIDEA16–2 и RFWKIDEA16–1, созданных на основе сети IDEA16–8 // Безопасность информации. –Киев. 2014. Том 20. №3. –с. 259–263.

39. Туйчиев Г.Н. О сети PES16–8, состоящей из восьми раундовых функций // Защита информации. –Киев. 2014. Том 16. №4. –с. 318–322.

40. Туйчиев Г.Н. О сетях PES16–4, PES16–2 и PES16–1, созданных на основе сети PES16–8 // Защита информации. –Киев. 2015. Том 17. №1. –с. 53–60.

41. Туйчиев Г.Н. О сетях RFWKPES16–8, RFWKPES16–4, RFWKPES16–2 и RFWKPES16–1, созданных на основе сети PES16–8 // Защита информации. –Киев. 2015. Том 17. №2. –с. 163–169.

42. Туйчиев Г.Н. Сеть PES32–16, состоящая из шестнадцати раундовых функции // Безопасность информации. –Киев. 2014. Том 20. №1. –с. 43–47.

43. Туйчиев Г.Н. О сетях PES32–8, PES32–4, PES32–2 и PES32–1, созданных на основе сети PES32–16 // Безопасность информации. –Киев. 2014. Том 20. №2. –с. 164–168.

44. Туйчиев Г.Н. Создание блочного алгоритма шифрования на основе сетей IDEA32–4 и RFWKIDEA32–4 с использованием преобразования алгоритма шифрования AES // Безопасность информации. –Киев. 2015. Том 21. №2. –с.148–158.

45. Tuychiev G. The encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 // «Information Security in the light of the Strategy Kazakhstan–2050»: proceedings III International scientific–practical conference (15–16 October 2015, Astana). –Astana. 2015. –pp. 355–371.

46. Tuychiev G. New encryption algorithm based on network PES8–1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security. 2015. Vol.4. №1. –pp.1–5.

47. Туйчиев Г.Н. Создание блочного алгоритма шифрования на основе сетей PES32–1 и RFWKPES32–1 с использованием преобразования алгоритма шифрования AES // Сборник научных работы научно–практической конференции «Актуальные вопросы обеспечения

кибернетической безопасности и защиты информации–CICSIS–2015». –Киев. 25–28 февраля 2015. –с.101–112.

48. Aripov M., Tuychiev G. Development block encryption algorithm based networks IDEA16–2 and RFWKIDEA16–2 using the transformation of encryption algorithm AES // «Information Security in the light of the Strategy Kazakhstan–2050»: proceedings III International scientific–practical conference (15–16 October 2015, Astana). – Astana. 2015. –pp.40–60

49. Туйчиев Г.Н. Алгоритмы блочного шифрования AES–PES16–2 и AES–RFWKPES16–2 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». –Ташкент. 2015 г.

50. Aripov M., Tuychiev G. The encryption algorithm AES–PES32–4 based on network PES32–4 // Transactions of the international scientific conference «Modern problems of applied mathematics and Information technologies–Al–Khorezmiy 2016». 2016. –Buchara. Vol № 2. –pp.28–34.

51. Программное обеспечение генерации стойких S–блоков размера 4x4 на основе конструкции Ниберга, 04.08.2015, № DGU 03291, Агентство по интеллектуальной собственности Республики Узбекистан.

52. Программное обеспечение генерации стойких S–блоков размера 8x8 на основе конструкции Ниберга, 04.08.2015, № DGU 03292, Агентство по интеллектуальной собственности Республики Узбекистан.

53. Алгоритмы блочного шифрования GOST28147–89–PES4–2, GOST28147–89–RFWKPES4–2, GOST28147–89–PES8–4 и GOST28147–89–RFWKPES8–4, 29.08.2015, № DGU 03321, Агентство по интеллектуальной собственности Республики Узбекистан.

54. Алгоритмы блочного шифрования AES–IDEA8–1, AES–RFWKIDEA8–1, AES–IDEA16–1, AES–RFWKIDEA16–1, AES–IDEA32–1, AES–RFWKIDEA32–1, AES–IDEA16–2, AES–RFWKIDEA16–2, AES–IDEA32–4 и AES–RFWKIDEA32–4, 21.04.2016, № DGU 03663, Агентство по интеллектуальной собственности Республики Узбекистан.

55. Алгоритмы блочного шифрования GOST28147–89–IDEA4–2, GOST28147–89–RFWKIDEA4–2, GOST28147–89–IDEA8–4, GOST28147–89 RFWKIDEA8–4, GOST28147–89–IDEA16–2, GOST28147–89–RFWKIDEA16–2, GOST28147–89–PES16–2 и GOST28147–89–RFWKPES16–2, 21.04.2016, № DGU 03664, Агентство по интеллектуальной собственности Республики Узбекистан.

56. Алгоритмы блочного шифрования AES–PES8–1, AES–RFWKPES8–1, AES–PES16–1, AES–RFWKPES16–1, AES–PES32–1, AES–RFWKPES32–1, AES–PES16–2, AES–RFWKPES16–2, AES–PES32–4 и AES–RFWKPES32–4, 30.12.2016, № DGU 04137, Агентство по интеллектуальной собственности Республики Узбекистан.

Автореферат «ЎзМУ хабарлари» журнали таҳририятида таҳрирдан ўтказилди
ва ўзбек, рус тилларидаги матнларни мослиги текширилди.
(11.09.2017 й).

Босишга рухсат этилди: 12.09.2017 йил
Бичими 60x45 $^{1}/_{8}$, «Times New Roman»
гарнитурада рақамли босма усулида босилди.
Шартли босма табоғи 4. Адади: 100. Буюртма: № 203.

Ўзбекистон Республикаси ИИВ Академияси,
100197, Тошкент, Интизор кўчаси, 68

«АКАДЕМИЯ НОШИРЛИК МАРКАЗИ»
Давлат унитар корхонасида чоп этилди.