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

САТТАРОВ АЛИЖОН БОЗОРБОЕВИЧ

ГОСТ 28147-89 АЛГОРИТМИ БАРДОШЛИЛИГИНИ ЧИЗИҚЛИ-ДИФФЕРЕНЦИАЛ ВА АЛГЕБРАИК КРИПТОТАҲЛИЛ УСУЛЛАРИ ЁРДАМИДА БАҲОЛАШ ВА БАРДОШЛИЛИГИ ЮҚОРИ БЎЛГАН ШИФР ЯРАТИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ФИЗИКА-МАТЕМАТИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

ТОШКЕНТ - 2019

УДК: 004.056.55

Физика-математика фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора (PhD) по физико-математическим наукам

Contents of dissertation abstract of doctor of philosophy (PhD) on physical-mathematical sciences

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

САТТАРОВ АЛИЖОН БОЗОРБОЕВИЧ

ГОСТ 28147-89 АЛГОРИТМИ БАРДОШЛИЛИГИНИ ЧИЗИҚЛИ-ДИФФЕРЕНЦИАЛ ВА АЛГЕБРАИК КРИПТОТАҲЛИЛ УСУЛЛАРИ ЁРДАМИДА БАҲОЛАШ ВА БАРДОШЛИЛИГИ ЮҚОРИ БЎЛГАН ШИФР ЯРАТИШ

05.01.05 - Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ФИЗИКА-МАТЕМАТИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

ТОШКЕНТ - 2019

Физика-математика фанлари бўйича фалсафа доктори (Doctor of Philosophy) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида №B2018.1.PhD/FM190 рақам билан рўйхатга олинган.

Диссертация Мирзо Улуғбек номидаги Ўзбекистон Миллий университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.ik-fizmat.nuu.uz) ва «ZiyoNet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий раҳбар:	**Абдурахимов Бахтиёр Файзиевич** физика-математика фанлари доктори, профессор
Расмий оппонентлар:	**Туйчиев Ғулом Нумонович** физика-математика фанлари доктори
	Худойқулов Зариф Тўрақулович техника фанлари бўйича фалсафа доктори (PhD)
Етакчи ташкилот:	**«UNICON.UZ» ДУК**

Диссертация ҳимояси Ўзбекистон Миллий университети ҳузуридаги DSc.27.06.2017.FM.01.02 рақамли Илмий кенгашнинг 2019 йил «_____»_____соат ___даги мажлисида бўлиб ўтади. (Манзил: 100174, Тошкент ш., Олмазор тумани, Университет кўчаси,4-уй. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz.)

Диссертация билан Ўзбекистон Миллий университетининг Ахборот-ресурс марказида танишиш мумкин (_____рақами билан рўйхатга олинган). (Манзил: 100174, Тошкент ш., Олмазор тумани, Университет кўчаси, 4-уй. Тел.: (+99871) 246-02-24).

Диссертация автореферати 2019 йил «____» _____куни тарқатилди.
(2019 йил «____» _____даги ___рақамли реестр баённомаси).

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

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

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

КИРИШ (фалсафа доктори (PhD) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳон миқёсида криптография ва криптотаҳлил муаммоларини ечишда шифрлаш алгоритмлари хоссаларини ўрганиш, уларни алгебраик ифодалаш, тарқатиш ва аралаштириш хусусиятига эга бўлган акслантиришларни ишлаб чиқиш етакчи ўринни эгалламоқда. Шунингдек, дунё мамлакатларида миллий стандарт шифрлаш алгоритмларини ишлаб чиқишга алоҳида эътибор қаратилмоқда. Шифрлаш алгоритми бардошлилигини баҳолаш ва криптографик акслантиришларни ишлаб чиқиш криптология, амалий математика ва объектга йўналтирилган дастурлаш каби соҳалардаги тадқиқотларнинг объектидир. Криптотаҳлил усуллари ва ҳисоблаш техникасининг ривожланиши криптотаҳлил масалаларини осон ечилишига ва шифрлаш алгоритмлари бардошлилигини пасайишига асос сифатида хизмат қилади. Шу сабабли, ахборот тизимларига таҳдидларни ошишини ҳисобга олган ҳолда, амалда фойдаланиб келинаётган шифрлаш алгоритмлари ишончлилигини баҳолаш ва бардошлилиги юқори бўлган янги шифрлаш алгоритмларини ишлаб чиқиш криптологиянинг муҳим вазифалардан бири бўлиб қолмоқда.

Ҳозирги кунда жаҳонда криптографик акслантиришлар ҳусусиятларини аниқлаш, шифрлаш алгоритмларини криптотаҳлил усуллари ёрдамида баҳолаш, юқори криптографик кўрсатгичли чизиқли ва чизиқсиз акслантиришлар ҳамда тезкор ва содда шифрлаш алгоритмларини ишлаб чиқиш криптологиянинг долзарб масалаларидан бири ҳисобланади. Мазкур ҳолда криптографик акслантиришларни алгебраик ифодалаш, уларнинг сонли характеристикаларини тадқиқ қилиш муҳим аҳамият касб этмоқда. Бу борада: миллий стандарт шифрлаш алгоритмлари бардошлилигини замонавий криптотаҳлил усуллари ёрдамида баҳолаш ва янги миллий шифрлаш алгоритмларини яратиш мақсадли илмий тадқиқотлардан ҳисобланади.

Мамлакатимизда фундаментал фанларнинг илмий ва амалий тадбиқига эга бўлган криптография ва криптотаҳлилнинг долзарб йўналишларига эътибор кўчайтирилди. Жумладан, криптографик акслантиришлар ва алгоритмларни ишлаб чиқиш соҳасида маълум ютуқларга эришилиб, ахборотларни узатиш ва қайта ишлашнинг ҳимояланган тизимларини яратишга алоҳида эътибор қаратилди. “Алгебра ва функционал анализ, Амалий математика ва математик моделлаштириш” фанларининг устувор йўналишлари бўйича халқаро стандартлар даражасида илмий тадқиқотлар олиб бориш асосий вазифалар ва фаолият йўналишлари этиб белгиланди[1]. Қарор ижросини таъминлашда шифрлаш алгоритмлари бардошлилигини сонли баҳолаш усулларини ишлаб чиқиш, бардошлилиги юқори бўлган шифр яратиш назариясини ривожлантириш муҳим аҳамиятга эга.

[1] Ўзбекистон Республикаси Вазирлар маҳкамасининг 2017 йил 18 майдаги «Ўзбекистон Республикаси Фанлар академиясининг янгидан ташкил этилган илмий тадқиқот муассасалари фаолиятини ташкил этиш тўғрисида»ги 292-сонли қарори.

Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги ПҚ-614–сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора–тадбирлари тўғрисида»ги Қарори, Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947 “Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисидаги” Фармони, 2017 йил 17 февралдаги ПҚ-2789-сон «Фанлар академияси фаолияти, илмий-тадқиқот ишларини ташкил этиш, бошқариш ва молиялаштиришни янада такомиллаштириш чора-тадбирлари тўғрисида»ги, 2017 йил 20 апрелдаги ПҚ-2909-сон «Олий таълим тизимини янада ривожлантириш чора-тадбирлари тўғрисида»ги ва 2018 йил 27 апрелдаги ПҚ-3682 “Инновацион ғоялар, технологиялар ва лойиҳаларни амалиётга жорий қилиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисидаги” қарорлари ҳамда мазкур фаолиятга тегишли бошқа норматив-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда ушбу диссертация тадқиқоти муайян даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологияларни ривожланишининг устувор йўналишларига боғлиқлиги. Диссертация республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Муаммонинг ўрганилганлик даражаси. ГОСТ 28147-89 шифрлаш алгоритмини турли криптотаҳлил усуллари ёрдамида баҳолаш масалалари бир қатор олимлар, жумладан: A.Dmukh, A.Shamir, B.Preneel, B.Schneier, D.Wagner, E.Fleischmann, G.Sekar, I.Dinur, J.Huhne, J.Kang, J.Kelsey, M.Gorski, M.Misztal, N.Courtois, N.Mouha, O.Dunkelman, O.Kara, S.Hong, S.Lee, S.Lucks, T.Isobe, W.Lee, Y.Ko, А.Алексейчук, В.Рудской, Г.Хоруженко, Е.Золотницкий, Е.Ищукова, Е.Маро, И.Кочетков, Л.Бабенко, М.Арипов, Р.Аллоев, Б.Абдурахимов, Ғ.Туйчиев, Ю.Пудовченко, Г.Жураев ва бошқаларнинг илмий ишларида кўриб чиқилган.

Шифрлаш алгоритми ва бардошли криптографик акслантиришлар ишлаб чиқиш масалалари билан боғлиқ тадқиқотлар бир қатор олимлар томонидан олиб борилган, жумладан: A.Youssef, B.Schneier, C.Adams, C.Shannon, G.Murtaza, I.Hussain, J.Nakahara, J.Rijmen, K.Chand, K.Gupta, K.Kazymyrov, K.Nyberg, M.Malik, M.Sajadieh, P.Freyre, P.Junod, S.Sim, А.Казимиров, А.Соколов, М.Арипов, М.Каримов, Б.Абдурахимов, Ғ.Туйчиев, Д.Акбаров, О.Ахмедова, П.Хасанов, Р.Олейников, Т.Чалкин, Д.Курьязов, Г.Жураев каби олимлар томонидан тадқиқ қилинган.

PES, IDEA ва AES шифрлаш алгоритмларини криптотаҳлил усуллари асосида баҳолаш, шифрлашда ягона алгоритмдан фойдаланиладиган Лай-Месси схемаси асосида шифрлаш алгоритмларини ишлаб чиқиш масалалари доирасида бир қатор олимлар: 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 X.Lai, J.L.Massey, М.Арипов, Ғ.Туйчиев, М.Бондаренко, А.Жуков, И.Горбенко, В.Долгов, Р.Олейников, В.Руженцевлар илмий изланишлар олиб боришган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Ўзбекистон Миллий университетининг «Амалий математика масалаларини ечишнинг алгоритмлари ва дастурий таъминоти» илмий-тадқиқот ишлари режасига мувофиқ бажарилган.

Тадқиқотнинг мақсади ГОСТ 28147-89 шифрлаш алгоритми бардошлилигини чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш ҳамда криптобардошлилиги юқори бўлган блокли симметрик шифрлаш алгоритмини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

блокли симметрик шифрлаш алгоритмларини яратиш ва уларни баҳолаш масалаларини ечиш;

ГОСТ 28147-89 шифрлаш алгоритмини чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш;

бардошлилиги юқори бўлган янги блокли симметрик шифрлаш алгоритмини яратиш

яратилган шифрлаш алгоритмининг бардошлилигини баҳолаш.

Тадқиқотнинг объекти ГОСТ 28147-89 шифрлаш алгоритми, чизиқли-дифференциал ва алгебраик криптотаҳлил ҳамда блокли симметрик шифрлаш алгоритмлари учун криптографик акслантиришлар қуриш усуллари ва объектга йўналтирилган дастурий воситалардан иборат.

Тадқиқотнинг предмети ГОСТ 28147-89 шифрлаш алгоритмини чизиқли-дифференциал ва алгебраик криптотаҳлил усули ёрдамида баҳолаш, максимал аралаштириш ва тарқатиш хусусиятига эга бўлган криптографик акслантиришлардан иборат.

Тадқиқотнинг усуллари. Тадқиқот ишида дастурлаш технологиялари, амалий криптография ва криптотаҳлил усуллари, Бул функцияларини қуриш усуллари, алгебраик тенгламалар системасини ечиш усуллари ва эҳтимоллар назарияси усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

криптографик акслантиришларни қуйи даражали алгебраик тенгламалар орқали ифодалаш усули ишлаб чиқилган;

SP тармоғига асосланган шифрлаш алгоритми яратилган ҳамда унинг бардошлилиги баҳоланган;

ўрин алмаштириш асосида максимал алгебраик иммунитетга ва юқори чизиқсизлик даражасига эга бўлган 8x8 ўлчамли S-блок қуриш алгоритми ишлаб чиқилган;

чекли майдонда аниқланган 8x8 ўлчамли тезкор ва инволютив MDS матрица ишлаб чиқилган;

SP тармоғига асосланган ва бардошлилиги юқори бўлган янги блокли симметрик шифрлаш дастури яратилган.

Тадқиқотнинг амалий натижалари чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш алгоритми ва дастурий таъминоти, криптографик акслантиришларни ишлаб чиқиш усуллари янги

шифр яратиш ва бардошлилигини баҳолаш масалаларини ечишда қўлланилган.

Тадқиқот натижаларининг ишончлилиги. Ҳисоблаш экспериментлари натижалари қатъий таққослаш усуллари орқали исботланган ва сонли тадқиқотлар натижалари билан тасдиқланган ҳамда математик мулоҳазаларнинг қатъийлиги билан асосланган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти шифрлаш алгоритмларини чизиқли-дифференциал ва алгебраик криптотаҳлил усули ёрдамида баҳолаш алгоритмлари, шунингдек, S-блок, MDS матрица, раунд калитларини ҳосил қилиш ва SP тармоғига асосланган шифрлаш алгоритмларини такомиллаштиришда қўлланилиши билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти шифрлаш алгоритмлари бардошлилигини аниқлашга, яратилган янги шифрлаш алгоритмлари орқали ахборотларни узатиш ва сақлаш жараёнида уларни ҳимоялашга имкон бериши билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. ГОСТ 28147-89 алгоритми бардошлилигини чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш ва бардошлилиги юқори бўлган шифр яратишда олинган илмий натижалар асосида:

ишлаб чиқилган S-блок қуриш алгоритми Ўзбекистон Республикаси Мудофаа вазирлиги тизимидаги “Zebra” дастурий таъминотида S-блокларни ишлаб чиқишда фойдаланилган (Радиоэлектрон тизимлар ва ахборот технологиялари марказининг 2019 йил 8 апрелдаги 20/2061-сонли маълумотномаси). Илмий натижанинг қўлланилиши ихтиёрий чекли сондаги турли хил S-блок жадвалларини қисқа вақт давомида ишлаб чиқишга имкон берган;

ишлаб чиқилган S-блок қуриш алгоритми Ўзбекистон Республикаси Мудофаа вазирлиги тизимидаги “Generator” дастурий таъминотида S-блокларни ишлаб чиқишда фойдаланилган (Радиоэлектрон тизимлар ва ахборот технологиялари марказининг 2019 йил 8 апрелдаги 20/2061-сонли маълумотномаси). Илмий натижанинг қўлланилиши юқори чизиқсизлик даражасига эга бўлган ўлчами 8x8 бўлган алмаштириш жадвалларини қисқа вақт давомида ишлаб чиқишга имкон берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 11 та, жумладан 6 та халқаро ва 5 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Тадқиқот мавзуси бўйича 17 та илмий иш чоп этилган, шулардан, Ўзбекистон Республикаси Олий аттестация комиссиясининг фалсафа доктори диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 5 та мақола, жумладан 2 таси хорижий ва 3 таси республика журналларида чоп этилган. Шунингдек, 1 та ўқув қўлланма нашр этилган ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш қисми, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва 16 та иловадан ташкил топган. Диссертациянинг ҳажми 110 бетни ташкил этган.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурати, тадқиқотнинг республика фан ва технологиялари ривожлантиришнинг устувор йўналишларига мос келиши асосланган. Диссертация мавзуси бўйича чет элдаги илмий тадқиқотларнинг қисқача маълумоти ва муаммонинг ўрганилганлик даражаси келтирилган, тадқиқотнинг мақсад, вазифалари шакллантирилган, унинг объекти ва предмети кўрсатилган, тадқиқотнинг амалий натижалари ва илмий янгиликлари баён қилинган, олинган натижаларнинг назарий ва амалий аҳамияти очиб берилган, тадқиқот натижаларининг қўлланилиши, диссертация тузилиши ва нашр қилинган илмий ишлар тўғрисида маълумотлар келтирилган.

Диссертациянинг **«Блокли симметрик шифрлаш алгоритмларини яратиш ва уларни баҳолашнинг замонавий тенденциялари»** деб номланган биринчи бобида блокли симметрик шифрлаш алгоритмларини яратиш бўйича турли давлатлар тажрибаси ва замонавий блокли симметрик шифрлаш алгоритмлари таҳлил қилинган. Блокли симметрик шифрлаш алгоритмларига қўлланилувчи асосий криптотаҳлил усуллари, уларнинг акслантиришларига қўйилувчи криптографик талаблар ва уларни яратиш ёндашувлари кўриб ўтилган.

XX аср 70 йиллари бошида К.Шеннон ва Х.Фейстел бошчилик қилган симметрик шифр тизимлари тадқиқига оид изланишлар натижасида Фейстел тармоғи деб аталувчи симметрик криптоалгоритм архитектураси яратилди. Ушбу тармоқ асосида ҳозиргача Lucifer, FEAL, Khufu, Khafre, LOKI, CAST, Blowfish, DES, ГОСТ 28147-89 блокли шифрлаш алгоритмлари яратилган.

2014 йил Россия Федерациясининг “Ахборотни криптографик ҳимоялаш” бўйича стандартлаштириш техник қўмитаси томонидан янги “Блокли шифрлаш алгоритми” стандарти лойиҳаси тақдим этилди. Ушбу стандарт лойиҳасида 2 та, яъни блок узунлиги 128 бит бўлган “Kuznyechik” алгоритми ва блок узунлиги 64 бит бўлган амалдаги “ГОСТ 28147-89” (Магма) алгоритми жорий этилган. Мазкур алгоритм лойиҳалари Россиянинг тегишли ташкилотлари томондан батафсил ўрганиб чиқилиб, ижобий фикрлар берилди ҳамда стандарт сифатида қабул қилинди.

2000 йил январ ойидан бошлаб 40 ой муддатга мўлжалланган NESSIE Европа криптолойиҳаси бўлиб ўтади. Мазкур лойиҳа очиқ танлов асосида Европанинг янги криптостандартларини танлаб олишга қаратилган Европа Комиссияси Дастурининг ахборот технологиялари жамияти (IST) доирасидаги илмий-тадқиқот лойиҳаси ҳисобланади. Танлов натижасида: Camellia, MYSTY, SHACAL ва AES алгоритмлари ғолиб сифатида танланган.

Блокли симметрик шифрлаш алгоритмларига замонавий криптотаҳлил усулларини қўллаш жараёни криптотаҳлилчи эга бўлган маълумотлар асосида

олиб борилади. Шунга мувофиқ, криптотаҳлил қуйидаги асосий турларга бўлинади: 1) Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида шифрматнни таҳлил қилиш. 2) Калит ҳақида маълумотга эга бўлиш мақсадида шифрматнларни таҳлил қилиш. 3) Калит ҳақида маълумотга эга бўлиш мақсадида очиқ матн билан таҳлил қилиш. 4) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган очиқ матн билан таҳлил қилиш. 5) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган шифр матнлар билан таҳлил қилиш. 6) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган матнлар ёрдамида таҳлил қилиш. 7) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган калитлар ёрдамида таҳлил қилиш.

Блокли симметрик шифрлаш алгоритмларига нисбатан юқорида келтирилган криптотаҳлил турларига асосланиб амалга оширилувчи қуйидаги замонавий криптотаҳлил усуллари мавжуд: чизиқли, дифференциал, чизиқли-дифференциал, интеграл, алгебраик ва бошқа.

Блокли симметрик шифрлаш алгоритмлари акслантиришларига қўйилувчи қуйидаги умумий криптографик талаблар мавжуд:

1. Ўрнига қўйиш (S-блок) акслантиришларининг регуляр бўлишлиги;
2. S-блок чиқиш битларини ифодаловчи буль функцияларнинг ($f_i(x)$) алгебраик чизиқсизлик даражасини юқори бўлишлиги;
3. $f_i(x)$ – буль функциянинг юқори корреляцион иммунитетлик (CI) даражаларига эга бўлишлиги;
4. $f_i(x)$ – функциянинг юқори тартибли қатъий лавин самарадорлик (SAC) ва тарқалиш тамойили кўрсаткичларига эга бўлишлиги;
5. $f_i(x)$– функциянинг юқори чизиқсизлик қийматига эга бўлишлиги.
6. S-блокнинг юқори чизиқсизлик қийматига эга бўлишлиги;
7. S-блокнинг юқори алгебраик иммунитетга эга бўлишлиги;
8. S-блок учун BIC (битлар боғлиқсизлиги тамойили) – қийматнинг нолга яқин бўлишлиги.

Санаб ўтилган мазкур талабларнинг ҳар бири шифрлаш алгоритмининг коррект ишлаши ва энг асосийси бардошлиликни таъминлаш учун асос бўлиб хизмат қилади. Жумладан, S-блок чизиқсизлик қийматининг юқори бўлиши алгоритмнинг чизиқли криптотаҳлил усулига, алгебраик иммунитетининг юқори бўлиши алгоритмнинг алгебраик криптотаҳлил усулига, регулярлик, корреляцион иммунитетлик, қатъий лавин самарадорлик ва тарқалиш тамойилларининг бажарилиши турли статистик криптотаҳлил усулларига бардошлиликни таъминлашга асос бўлади.

Диссертациянинг **«ГОСТ 28147-89 алгоритми бардошлилигини чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолашни тадқиқ этиш»** деб номланган иккинчи бобида ГОСТ 28147-89 алгоритмини чизиқли-дифференциал (ЧДК) ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш масалалари ва уларнинг ечимлари, баҳолашдан олинган натижалар келтирилган.

ЧДК усулнинг асосий моҳияти чизиқли (ЧК) ва дифференциал (ДК) криптотаҳлил усулларини умумлаштиришга асосланган. ГОСТ 28147-89 алгоритмини ушбу усулга баҳолаш учун қуйидаги масалалар ҳал этиш лозим:

1) Раундлар сонининг ДК ва ЧК усулларига тақсимланиши;

2) Керакли аппроксимация тенгламаларини тузиш;

3) Самарадорлиги юқори бўлган айирма кўринишини аниқлаш;

4) Сўнгги раунд калит қиймати вариантларини аниқлаш.

Тақсимот – шифрлаш *алгоритми раундлар сонига* ҳамда *ДК ва ЧК усулларининг самарадорлигига* боғлиқ тарзда аниқланади. Ушбу тақсимотни *Taqsimot([NДК], [NЧК])* – функция кўринишида белгилаймиз, бу ерда: *Taqsimot()* – тақсимот функциясини, *NДК (NДК=$n_1,n_2,n_3,\ldots . n_i \in N$)* – ДК усули қўлланилувчи раундларни, *NЧК (NЧК=$n_1,n_2,n_3,\ldots . n_i \in N$)* – ЧК усули қўлланилувчи раундларни, *len(NДК)* – ДК (ЧК) усули қўлланилган умумий раундлар сонини, *[-]* – ДК (ЧК) усули қўлланилмаганлигини ифодалайди. Ушбу функция учун қуйидагилар ўринли.

Тасдиқ 1. R (R>2) – раундли ГОСТ 28147-89 алгоритми учун *len[NДК]+len[NЧК]+2=R* тенглик ўринли.

Тасдиқ 2. ГОСТ 28147-89 алгоритмини ЧДК усули ёрдамида баҳолаш жараёнида ЧК усули қўлланувчи умумий раундлар сони 4 тадан ошмайди, яъни *len*[*NЧК*]≤3 ўринли.

1-жадвалда ЧК усулини *len*(*NЧК*)≤*3* раундларга қўллаб, алгоритмининг сўнгги раундида фойдаланилган қисм калитларни аниқлаш имкониятини берадиган, юқори четланишли аппроксимация тенгламалари ва уларни қисм калит билан боғлиқлиги келтирилган.

1-жадвал

Керакли аппроксимация тенгламалари

Изланаётган қисм калит	*S* блок	Аппроксимация тенгламаси	Четланиш қиймати (*Δ*)	Эҳтимоллик қиймати (*p*)
K_1	S_7	$\Delta X_{25} \oplus \Delta Y_{17}=0$	$\Delta=3/4$	$P=1/8$
K_2	S_7	$\Delta X_{28} \oplus \Delta Y_{14}=0$	$\Delta=1/2$	$P=3/4$
K_3	S_1	$\Delta X_1 \oplus \Delta Y_{25}=0$	$\Delta=1/2$	$P=3/4$
K_4	S_1	$\Delta X_4 \oplus \Delta Y_{24}=0$	$\Delta=1/2$	$P=3/4$
K_5	S_2	$\Delta X_8 \oplus \Delta Y_{29}=0$	$\Delta=1/2$	$P=3/4$
K_6	S_3	$\Delta X_{10} \oplus \Delta Y_{31}=0$	$\Delta=1/2$	$P=1/4$
K_7	S_4	$\Delta X_{14} \oplus \Delta Y_3=0$	$\Delta=1/2$	$P=1/4$
K_8	S_5	$\Delta X_{18} \oplus \Delta Y_7 \oplus \Delta Y_9=0$	$\Delta=1/2$	$P=1/4$

Самарадорлиги юқори бўлган айирма қийматини аниқлаш раундлар сонига ва раунд акслантиришларининг битларни тарқатиш хусусиятига боғлиқ ҳолда аниқланади. Қуйидаги теорема исботланган:

Теорема 1. Айтайлик, *M* ($M=m_1||m_2||m_3||\ldots||m_{64}$) – 64 битли очиқ матн, *C* ($C=c_1||c_2||c_3||\ldots||c_{64}$) – *M* очиқ матнни 256 битли *K* ($K=k_1||k_2||k_3||\ldots||k_{256}$) – калит ёрдамида раундлар сони *r* ($r\in\{1,2,3,\ldots32\}$) та бўлган ГОСТ 28147-89 алгоритми орқали шифрлаш натижасида ҳосил қилинган 64 битли шифрматн, *w* – эса бирор c_i ($i\in\{1,2,3,\ldots64\}$) нинг қийматини ўзгаришига таъсир этувчи очиқ матн битлари сони бўлсин. Агар $r\geq8$ бўлса, у ҳолда *i* нинг исталган қийматидаги c_i учун $w=64$ тенглик ўринли.

ГОСТ 28147-89 алгоритмини ЧДК усули ёрдамида баҳолашдан олинган натижаларга кўра, қуйидагилар ўринли.

Тасдиқ 3. ГОСТ 28147-89 алгоритмини ЧДК усули ёрдамида баҳолаш жараёнида ДК усули қўлланувчи умумий раундлар сони 9 тадан ошмайди, яъни $len[НДК] \leq 9$ ўринли.

Тасдиқ 4. Раундлар сони 12 ва ундан юқори бўлган ГОСТ 28147-89 алгоритми ЧДК усулига амалий бардошли.

ГОСТ 2814789 шифрлаш алгоритмига алгебраик криптотаҳлил усулини қўллаш жараёнида алгоритмни тенгламалар системаси орқали ифодалаш қуйидаги масалаларни ечишни талаб этади:

a) шифрлаш алгоритмини декомпозициялаш;

b) ҳар бир элементни алгебраик ифодалаш;

c) ҳар бир элементнинг кириши ва чиқишини бошқа элементлар ҳамда калит, очиқ матн ва шифрматн битлари билан боғлаш.

ГОСТ 2814789 алгоритми S-блокларини ифодаловчи $deg \leq 2$ бўлган тенгламалар системасини қуриш учун ишлаб чиқилган алгоритм ($n=4$):

1. S блок акслантириши учун текширув жадвали шакллантирилсин.

2. Текширув жадвалининг ҳар бир чиқувчи $f_1, f_2, \ldots, f_k$ $(k=(3n^2+n)/2)$ – функцияларига нисбатан АНФ қурилсин.

3. Агарда $2n^2+n+1>2^n$ ўринли бўлса "барча АНФларнинг тегишли комбинацияларидан фойдаланиб $deg \leq 2$ шарт бажарилувчи m та *$(2n^2+n-2^n+1 \leq m \leq k)$ чизиқли эркли тенгламалар шакллантирилсин" акс ҳолда тамомлансин.*

4. Барча $deg \leq 2$ бўлган тенгламалар натижавий тенгламалар системаси сифатида эълон қилинсин ва тамомлансин.

Шифрлаш алгоритмида фойдаланилган раунд калитларини қўшиш акслантириши ($z=F(x,k)$) учун қуйидаги тасдиқлар ўринли:

Тасдиқ 5. $z=F(x,k)$ акслантиришининг ҳар бир чиқувчи z_i-функцияси учун $\deg(z_i)=i$ тенглик ўринли.

Тасдиқ 6. $z=F(x,k)$ акслантиришга нисбатан $p=0{,}75$ эҳтимоллик билан бажарилувчи қуйидаги $z_i=x_i \oplus k_i \oplus k_{i-1}$, $z_i=x_i \oplus x_{i-1} \oplus k_i$ $(2 \leq i \leq 32)$ тенгламалар ўринли ва криптотаҳлил учун энг самаралидир.

ГОСТ 28147-89 алгоритмини алгебраик криптотаҳлил усули ёрамида баҳолашдан олинган натижаларга кўра қуйидаги тасдиқ ўринли:

Тасдиқ 7. Раундлар сони 5 ва ундан юқори бўлган ГОСТ 28147-89 алгоритми алгебраик критотаҳлил усулига амалий бардошли.

Диссертациянинг **«Блокли симметрик шифрлаш алгоритмини яратиш»** деб номланган учинчи бобида SP тармоғи асосида ишлаб чиқилган блокли симметрик шифрлаш алгоритми, унинг криптографик акслантиришлар ва раунд калитларини ҳосил қилиш жараёнлари келтирилган.

SP тармоғига асосланган янги шифрлаш алгоритми акслантиришларини ишлаб чиқишда максимал "аралаштириш" ва "тарқатиш" хусусиятига эга, шунингдек, умумий криптографик талабларни қаноатлантирувчи, криптографик кўрсатгичлари юқори ва замонавий криптотаҳлил усулларига бардошли бўлган, соддалик ва тезкорлик тамойилларига асосланилди.

Аралаштириш хусусиятини таъминловчи асосий чизиқсиз акслантириш сифатида (8x8)-ўлчамли 2 та S-блок ишлаб чиқилди. Ушбу S-блокларнинг криптографик кўрсатгичлари 2 ва 3-жадвалда келтирилган.

2-жадвал

S_1(8x8)-блокнинг криптографик кўрсатгичлари

Криптографик кўрсатгичлар	**S_1(8x8)-блок**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
баланслашганлик	+	+	+	+	+	+	+	+
регулярлик	+							
deg(f)	7	7	7	7	7	7	7	7
N(f)	112	112	112	112	112	112	112	112
N(S)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	8	8	4	6	8	8	8	6
δ	4							
D(S)	878220							
Заиф нуқта	–							
AI(S)	2							

S_1(8x8)-блок шифрлаш алгоритмини чизиқли, дифференциал, чизиқли-дифференциал криптотаҳлил усулларига бардошлилигини ошишини таъминлайди. Ушбу S-блок Ниберг конструкциясияси ёрдамида, *D*(*S*) параметри юқори бўлишлилик ва заиф нуқтага эга бўлмаслилик мезонлари асосида яратилди.

3-жадвал

S_2(8x8)-блокнинг криптографик кўрсатгичлари

Криптографик кўрсатгичлар	**S_2(8x8)-блок**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
баланслашганлик	+	+	+	+	+	+	+	+
регулярлик	+							
deg(f)	7	7	7	7	7	7	7	7
N(f)	106	108	108	108	106	110	106	106
N(S)	104							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	8	10	6	8	8	8	12	8
δ	8							
D(S)	31050							
Заиф нуқта	–							
AI(S)	3							
T(S)	441							

S_2(8x8)-блок шифрлаш алгоритмини алгебраик ва бошқа криптотаҳлил усулларига бардошлилигини ошишини таъминлайди.

Ушбу S-блокни ишлаб чиқиш алгоритми қуйидагича яратилди ($S(8x8)_{max}$ – блок учун $N(S)$=112 ўринли):

1. $S(8x8)=S(8x8)_{max}$.

2. *S(8x8)-блокни тасодифий 39 та элементи ўзаро ўрин алмаштирилсин.*
3. *2-қадам натижасида ҳосил қилинган S(8x8)-блокнинг N(S) ва δ параметр қийматлари аниқлансин.*
4. *Агар N(S)<104 ёки δ>8 бўлса 1-қадамга ўтилсин.*
5. *2-қадам натижасида ҳосил қилинган S(8x8)-блокнинг AI(S) ва N_{TS} параметр қийматлари аниқлансин.*
6. *Агар AI(S)≠3 ёки N_{TS}≠441 бўлса 1-қадамга ўтилсин.*
7. *S(8x8)-блок чиқувчи маълумот сифатида эълон қилинсин.*

Тарқатиш хусусиятини таъминловчи асосий акслантириш сифатида қуйида келтирилган (8x8)-тартибли *MDS* (Maximum Distance Separable) матрицани (8x*w*)-тартибли матрицага $GF(2^8)/\varphi(x)$ ($\varphi(x)=x^8\oplus x^7\oplus x^6\oplus x\oplus 1$) – чекли майдонда кўпайтириш амалидан фойдаланилди.

$$MDS=\begin{bmatrix}1,2,3,4,5,112,145,225\\2,1,4,3,112,5,225,145\\3,4,1,2,145,225,5,112\\4,3,2,1,225,145,112,5\\5,112,145,225,1,2,3,4\\112,5,225,145,2,1,4,3\\145,225,5,112,3,4,1,2\\225,145,112,5,4,3,2,1\end{bmatrix}$$

Тасдиқ 8. Берилган матрица инволютив ва тезкор (енгил) матрица.

Раунд калитлари 2^n ($16\le n\le 64$) модул бўйича қўшилиб (айирилиб), ушбу амал шифрлаш алгоритмининг интеграл ва аксарият криптотаҳлил усулига бардошлилигини оширади.

Шифрлаш алгоритми 128, 256, 384 ва 512 бит узунликдаги маълумот блокини мос равишда 8, 10, 12, 14 та раунд ёрдамида *B*, *T*, *S* ва *K* деб номланувчи акслантиришлардан фойдаланган ҳолда шифрлаш ва очиқ матнга ўгириш имкониятига эга бўлиб, блок узунлигидан кичик бўлмаган 128, 256, 384 ва 512 бит узунликдаги махфий калитдан фойдаланиши мумкин.

Умумий ҳолда, "*r*" раундли алгоритм учун қуйидаги шифрлаш ва очиқ матнга ўгириш формулалари ўринли:

$$C=K(...K(S(T(B(K(S(T(B(K(M,Rk_0)))),Rk_1))))),Rk_2)...,Rk_r);$$

$$M=K^{-1}(...K^{-1}(B^{-1}(T(S^{-1}(K^{-1}(B^{-1}(T(S^{-1}(K^{-1}(M,Rk_r))))),Rk_{r-1}))))),Rk_{r-2})...,Rk_0)$$

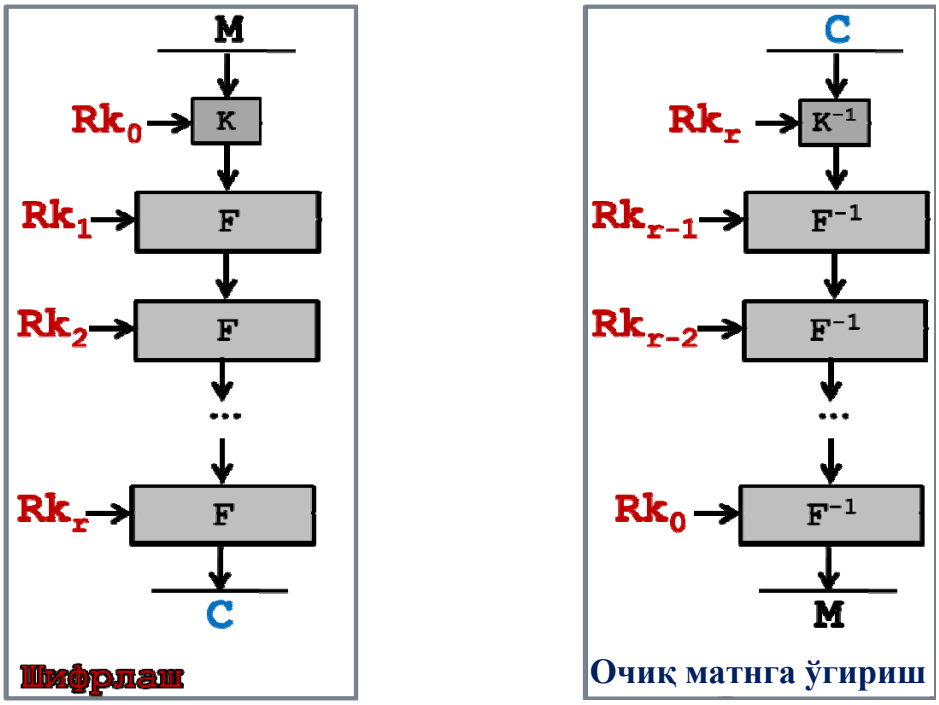
Тасдиқ 9. *B*, *T*, *S*, *K* акслантиришларидан фойдаланиб 2-раунддан сўнг максимал лавин самарадорликка эришилади.

Раунд калитларини ҳосил қилиш функциясини ишлаб чиқишда қуйидаги талабларнинг бажарилишига асосланилди:

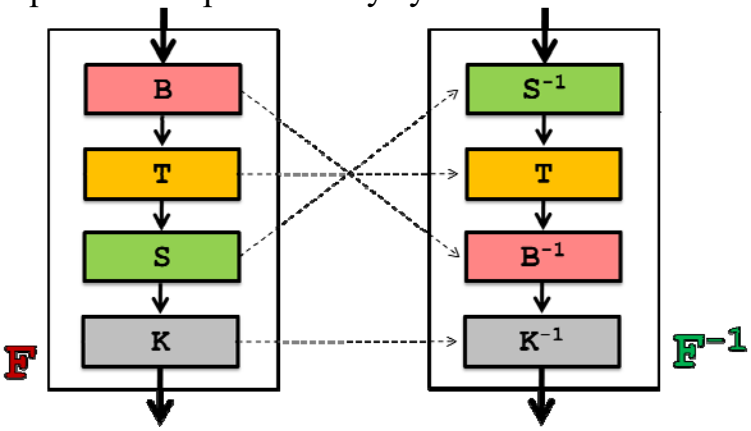
- бир томонлилик (қайтмас);
- турли узунликдаги кирувчи ва чиқувчи қийматларга мослашувчанлик.

Махфий калит асосида раунд калитларини ҳосил қилиш функцияси (φ) учун қуйидаги теорема ўринли.

Теорема 2. Агар *key* – маҳфий калит, Rk_i – эса *i* ($i\ge 0$) – раунд калити бўлса, у ҳолда қуйидаги ифода ўринли: $Rk_i = \varphi(key, i)$



1-расм. Алгоритмнинг умумий ишлаш схемаси



2-расм. Раунд функциясининг умумий ишлаш схемаси

Диссертациянинг **«Яратилган шифрлаш алгоритми криптобардошлилигини баҳолаш»** деб номланган тўртинчи бобида, яратилган шифрлаш алгоритмини бардошлилиги ва турли криптографик кўрсатгичлари баҳоланган.

Яратилган шифрлаш алгоритмига дифференциал криптотаҳлил усулини қўллаш учун экспериментал тарзда топилган оптимал айирмалар 4-жадвалда келтирилган.

4-жадвал

128 бит блок узунлигига нисбатан топилган оптимал айирмалар

***r*-рауннддан сўнг**	**Талаб этилувчи матнлар сони**	**Айирма вариантлари** (16 лик саноқ тизимида)
3	2^{127}	00000000002300660000000000000000
4	2^{219}	0000002D000000000000000000000C0
5	2^{303}	00000000000000EC00000000000000EC
6	2^{393}	0000000000000000EF00270000000000
7	2^{479}	00000000000000C000000000000000EC
8	2^{570}	00000000000000EC00000000000000C0

Шифрлаш алгоритми бардошлилигини дифференциал криптотаҳлил усули ёрдамида баҳолаш натижасига кўра аниқландики, умумий ҳолда блок узунлиги l бит бўлган алгоритм криптотаҳлили учун талаб этилувчи матнлар сони ҳар бир раунддан сўнг $\approx 2^{91\bullet\frac{l}{128}}$ га ошиши мумкин.

Тасдиқ 10. Яратилган алгоритм дифференциал криптотаҳлил усулига 4-раунддан сўнг амалий бардошли ҳисобланади.

Алгоритмга чизиқли криптотаҳлил усулини қўллаш учун шакллантирилган тенгламаларга нисбатан қуйидагилар ўринли.

$S_1(8,8)$-блокка нисбатан энг юқори четланишга эга бўлган чизиқли тенгламалар 255 та бўлиб, уларнинг четланиш қиймати 0,125 га тенг.

$S_2(8,8)$-блокка нисбатан энг юқори четланишга эга бўлган чизиқли тенгламалар эса 33 та бўлиб, уларнинг четланиш қиймати 0,1875 га тенг.

MDS матрицага кўпайтириш акслантиришига кирувчи битлар (x_0, x_1, x_2,…, x_{63}) ва ундан чиқувчи битлар (y_0, y_1, y_2,…, y_7) учун p=1 эҳтимоллик билан бажарилувчи қуйидаги намунавий тенглама ўринли:

$$y_0=x_0\oplus x_8\oplus x_9\oplus x_{17}\oplus x_{25}\oplus x_{26}\oplus x_{32}\oplus x_{33}\oplus x_{34}\oplus x_{46}\oplus x_{54}\oplus x_{55}\oplus x_{56}$$

Тасдиқ 11. Яратилган алгоритм чизиқли криптотаҳлил усулига 3-раунддан сўнг амалий бардошли.

Алгебраик криптотаҳлил усулига баҳолаш натижаларига мувофиқ қуйидаги тасдиқ ўринли.

Тасдиқ 12. Яратилган алгоритм алгебраик криптотаҳлил усулига 3-раунддан сўнг амалий бардошли.

ХУЛОСА

Диссертация иши ГОСТ 28147-89 алгоритми бардошлилигини чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш ва бардошлилиги юқори бўлган блокли симметрик шифрлаш алгоритмини яратишга бағишланган.

Тадқиқотнинг асосий натижалари қуйидагилардан иборат:

1. ГОСТ 28147-89 алгоритмига чизиқли-дифференциал ва алгебраик криптотаҳлил усуллари қўлланилган ва алгоритм бардошлилиги баҳоланган.
2. Криптографик акслантиришларни қуйи даражали алгебраик тенгламалар орқали ифодалаш усули ишлаб чиқилган.
3. Максимал алгебраик иммунитет ва юқори чизиқсизлик қийматига эга бўлган S-блок жадвалини ишлаб чиқиш алгоритми яратилган.
4. SP тармоғига асосланган ҳамда ўзгарувчан блок ва калит узунликларида ишлаши мумкин бўлган янги шифрлаш алгоритми яратилган.
5. Шифрлаш акслантиришларидан фойдаланган ҳолда раунд калитларини генерациялаш алгоритми яратилган.
6. Янги яратилган шифрлаш алгоритмининг бардошлилиги дифференциал, чизиқли ва алгебраик криптотаҳлил усуллари асосида баҳоланган.

НАУЧНЫЙ СОВЕТ DSc.27.06.2017.FM.01.02
ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ
НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

САТТАРОВ АЛИЖОН БОЗОРБОЕВИЧ

ОЦЕНКА СТОЙКОСТИ АЛГОРИТМА ГОСТ 28147-89 ЛИНЕЙНО-ДИФФЕРЕНЦИАЛЬНЫМ И АЛГЕБРАИЧЕСКИМ МЕТОДАМИ КРИПТОАНАЛИЗА И РАЗРАБОТКА ШИФРА С ПОВЫШЕННОЙ СТОЙКОСТЬЮ

05.01.05 – Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА ФИЛОСОФИИ (PhD)
ПО ФИЗИКО-МАТЕМАТИЧЕСКИМ НАУКАМ

Ташкент-2019

Тема диссертации доктора философии (PhD) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2018.1.PhD/FM190.

Диссертация выполнена в Национальном Университете Узбекистана имени М Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (http://ik-fizmat.nuu.uz) и на Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
Официальные оппоненты:	**Туйчиев Гулом Нумонович** доктор физико-математических наук
	Худойкулов Зариф Туракулович доктора философии по техническим наукам (PhD)
Ведущая организация:	**ГУП «UNICON.UZ»**

Защита диссертации состоится «____» _____2019 года в ____ часов на заседании Научного совета DSc.27.06.2017.FM.01.02 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за №____). (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 246-02-24).

Автореферат диссертации разослан «____» _____2019 года.
(протокол рассылки №_____ от «____» _____2019 года).

А.Р.Марахимов
Председатель Научного совета по присуждению ученых степеней, д.ф.-м.н., профессор

З.Р.Рахмонов
Ученый секретарь Научного совета по присуждению ученых степеней, д.ф.-м.н.

Р.Д.Алоев
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.ф.-м.н., профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность диссертации. На сегодняшний день изучение свойст алгоритмов шифрования, их алгебраического представления, разработка преобразований, имеющих свойства рассеивания и перемешивания, для решения проблем криптографии и криптоанализа, занимают важную роль во всем мире. Также государствами уделяется особое внимание разработке националного стандарта алгоритма шифрования. Оценка стойкости криптографического алгоритма и разработка криптографического преобразования является объектом исследований в таких областях, как криптология, прикладная математика и объектно-ориентированное программирование. Развитие методов криптоанализа и вычислительных технологий служит основой для простых решений задач криптоанализа и оценки стойкости алгоритмов шифрования. В этой связи одной из важных задач криптологии является оценка надежности алгоритмов, которые используются на практике, и разработка новых алгоритмов шифрования с высокой степенью стойкости.

В настоящее время определение свойств криптографического преобразования, оценка алгоритмов шифрования с помощью методов криптоанализа, разработка линейных и нелинейных преобразований, а также быстрых и простых алгоритмов шифрования является одной из актуальных проблем криптологии во всём мире. Важно исследование алгебраического выражения (представления) криптографических преобразований и их количественных характеристик. В этой связи: оценка стойкости алгоритмов шифрования национального стандарта с помощью современных методов криптоанализа и создание новых национальных алгоритмов шифрования являются целенаправленными научными исследованиями.

В нашей стране усилено внимание на важные аспекты криптологиии, которые имеют научное и практическое применение. В частности, особое внимание было уделено достижению успехов в области разработки криптографического преобразования и алгоритмов, а также созданию защищённых (безопасных) систем для передачи и обработки данных. Проведение научных исследований на уровне международных стандартов по приоритетным направлениям «Алгебра и функциональный анализ, Прикладная математика и математическое моделирование» являются основными задачами и направлениями деятельности[1]. Для обеспечения исполнения данного постановления важно развивать теорию разработки методов количественной оценки стойкости алгоритмов шифрования и создания шифра с высокой степенью стойкости.

Данная диссертация, в определенной степени нацелена на решение задач, обозначенных в Постановлениях Президента Республики Узбекистан № ПП-614 «О мерах по организации криптографической защиты

[1] Постановление Кабинета Министров Республики Узбекистан №292 «О мерах по организации деятельности вновь созданных научно-исследовательских учреждений академии наук Республики Узбекистан» от 18 мая 207 года.

информации в Республике Узбекистан» от 3 апреля 2007 года, № УП-4947 от 7 февраля 2017 года «О стратегии действия по дальнейшему развитию Республики Узбекистан», № УП-2789 от 17 февраля 2017 года «О мерах по дальнейшему совершенствованию деятельности Академии наук, организации, управления и финансирования научно-исследовательской деятельности», № ПП-2909 от 20 апреля 2017 года «О мерах по дальнейшему развитию системы высшего образования» и № ПП-3682 от 27 апреля 2018 года «О мерах по дальнейшему совершенствованию системы практического внедрения инновационных идей, технологий и проектов», а также в других нормативно-правовых актах по данной деятельности.

Соответствие исследований приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствии с приоритетными направлениями развития науки и технологий в Республике Узбекистан IV. «Информатизация и развитие информационно–коммуникационных технологий».

Степень изученности проблемы. Вопросы оценки алгоритма шифрования ГОСТ 28147-89 разными методами криптоанализа рассмотрены в научных трудах ряда ученых: A.Dmukh, A.Shamir, B.Preneel, B.Schneier, D.Wagner, E.Fleischmann, G.Sekar, I.Dinur, J.Huhne, J.Kang, J.Kelsey, M.Gorski, M.Misztal, N.Courtois, N.Mouha, O.Dunkelman, O.Kara, S.Hong, S.Lee, S.Lucks, T.Isobe, W.Lee, Y.Ko, А.Алексейчук, В.Рудской, Г.Хоруженко, Е.Золотницкий, Е.Ищукова, Е.Маро, И.Кочетков, Л.Бабенко, М.Арипов, Р.Аллоев, Б.Абдурахимов, Г.Туйчиев, Ю.Пудовченко, Г.Жураев и других.

Вопросам разработки алгоритмов шифрования и оценки стойкости криптографических преобразований посвящены работы A.Youssef, B.Schneier, C.Adams, C.Shannon, G.Murtaza, I.Hussain, J.Nakahara, J.Rijmen, K.Chand, K.Gupta, K.Kazymyrov, K.Nyberg, M.Malik, M.Sajadieh, P.Freyre, P.Junod, S.Sim, А.Казимиров, А.Соколов, М.Арипов, М.Каримов, Б.Абдурахимов, Г.Туйчиев, Д.Акбаров, О.Ахмедова, П.Хасанов, Р.Олейников, Т.Чалкин, Д.Курьязов, Г.Жураев и других ученых.

Вопросы оценки стойкости алгоритмов шифрования PES, IDEA и AES методами криптоанализа, разработка алгоритмов шифрования на основе схемы Лай–Месси, использующей один и тот же алгоритм при шифровании, провели научных исследований ряд ученых: 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 X.Lai, J.L.Massey, М.Арипов, Ғ.Туйчиев, М.Бондаренко, А.Жуков, И.Горбенко, В.Долгов, Р.Олейников, В.Руженцев и других.

Связь темы диссертации с научно-исследовательскими работами высшего учебного заведения, в которой выполнялась диссертация. Работа выполнена в соответствии плановой тематикой «Алгоритмы и программное обеспечение решения задач прикладной математики» Национального университета Узбекистана.

Целью исследования является оценка криптостойкости алгоритма шифрования ГОСТ 28147-89 линейно-дифференциальным и алгебраическим

методами криптоанализа, а также разработка алгоритма блочно-симметричного шифрования с повышенной криптостойкостью.

Задачи исследования состоят в следующем:

решение задач по созданию алгоритмов блочно-симметричного шифрования и их оценки;

оценка алгоритма шифрования ГОСТ 28147-89 с использованием линейно-дифференциального и алгебраического методов криптоанализа;

создание нового блочно-симметричного алгоритма шифрования с высокой стойкостью;

оценка стойкости созданного алгоритма шифрования.

Объектом исследования является алгоритм шифрования ГОСТ 28147-89, линейно-дифференциальный и алгебраический криптоанализ, а также методы построения криптографических преобразований для алгоритмов блочно-симметричного шифрования и объектно-ориентированные программные средства.

Предметом исследования является оценка стойкости алгоритма шифрования ГОСТ 28147-89 на линейно-дифференциальный и алгебраический криптоанализ, разработка криптографических преобразований, которые имеют свойства максимального рассеивания и перемешивания.

Методы исследования. В работе используются методы программирования, прикладной криптографии и криптоанализа, построения булевых функций, решения систем алгебраических уравнений и теории вероятностей.

Научная новизна исследования заключается в следующем:

разработан метод описания криптографических преобразований при помощи алгебраических уравнений нижней степени;

разработан алгоритм шифрования, основанный на сети SP, а также оценена его стойкость;

разработан алгоритм построения S-блока размером 8x8 с максимальной алгебраическим иммунитетом и высокой степенью нелинейности;

разработана быстрая и инволютивная матрица MDS, размером 8x8, определенная над конечным полем;

разработано программное обеспечение нового блочно-симметричного алгоритма шифрования с высокой степенью стойкости, основанного на сети SP.

Практические результаты – алгоритмы и программное обеспечение оценки с помощью линейно-дифференциального и алгебраического методов криптоанализа, методы разработки криптографических преобразований применены в решении задач по созданию нового шифра и оценки стойкости.

Достоверность результатов исследования. Достоверность результатов вычислительных экспериментов доказана методами строгого сравнения и утверждена результатами вычислительных исследований, а также обоснована строгостью математических рассуждений.

Научная и практическая значимость результатов исследования.

Научное значение результатов исследования заключается в том, что его можно использовать в усовершенствовании алгоритмов оценки стойкости алгоритмов шифрования методами линейно-дифференциального и алгебраического криптоанализа, а также при создании S-блока, матрицы MDS, алгоритма генерации раундовых ключей и шифрования на основе сети SP.

Практическая значимость диссертации состоит в том, что результаты позволяют определить стойкость алгоритмов шифрования, защитить информацию в процессе их передачи и хранения посредством нового алгоритма шифрования.

Внедрение результатов исследования. Научные результаты по оценке стойкости алгоритма ГОСТ 28147-89 линейно-дифференциальным и алгебраическим методами криптоанализа и разработка шифра с повышенной стойкостью внедрены в практику по следующим направлениям:

Алгоритм построения S-блоков применен для генерации S-блоков в программном обеспечении «Zebra», используемом в системе Министерства обороны Республики Узбекистан (справка Центра радиоэлектронных систем и информационных технологии от 8 апреля 2019 года рег. №20/2061). Внедрение научного результата предоставило возможность генерации произвольного ограниченного количества стойких S-блоков в короткое время.

Алгоритм построения S-блоков применен для генерации S-блоков в программном обеспечении «Generator», используемом в системе Министерства обороны Республики Узбекистан (справка Центра радиоэлектронных систем и информационных технологии от 8 апреля 2019 года рег. №20/2061). Внедрение научного результата предоставило возможность генерации произвольного ограниченного количества стойких таблиц замены размером 8x8, имеющих высокую степень нелинейности в короткое время.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 11 научно-практических конференциях, в том числе на 6 международных и 5 республиканских.

Публикация результатов исследования. По теме диссертации опубликовано 17 научных работ, из них 5 входят в перечень научных изданий, предложенных Высшей аттестационной комиссией Республики Узбекистан для защиты диссертаций доктора философии, из них 2 опубликованы в зарубежных журналах и 3 в республиканских научных изданиях. Издано 1 учебное пособие и получены 3 свидетельства о регистрации программных средств для ЭВМ.

Структура и объем диссертации: Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и 16 приложений. Объем диссертации составляет 110 страницы.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и востребованность темы диссертации, определено соответствие исследования приоритетным направлениям развития науки и технологий республики. Приведен обзор зарубежных научных исследований по теме диссертации и оценена степень изученности проблемы, сформулированы цели и задачи, выявлены объект и предмет исследования, изложены научная новизна и практические результаты исследования, раскрыта теоретическая и практическая значимость полученных результатов, даны сведения о внедрении результатов исследования, об опубликованных работах и о структуре диссертации.

В первой главе диссертации **«Современные тенденции создания блочно-симметричных алгоритмов шифрования и их оценки»** проанализирован опыт разных стран по созданию блочно-симметричных алгоритмов шифрования и современные блочно-симметричные алгоритмы шифрования. Рассмотрены основные методы криптоанализа, применяемые для алгоритмов блочно-симметричного шифрования, криптографические требования к их преобразованию и подходы к их созданию.

В начале 70-х годов XX века по результатам исследований по симметричным системам шифрования, проведенные под руководством К.Шеннона и Х.Фейстела, была создана архитектура симметрическая криптоалгоритма под названием сеть Фейстеля. На основе этой сети на сегодняшний день были созданы блочные алгоритмы шифрования Lucifer, FEAL, Khufu, Khafre, LOKI, CAST, Blowfish, DES, ГОСТ 28147-89.

В 2014 году Технический комитет по стандартизации «Криптографической защиты информации» Российской Федерации представил новый проект стандарта «Алгоритм блочного шифрования». В данном проекте стандарта были введены 2 алгоритма: «Kuznyechik» с длиной блока 128 бит и действующий алгоритм «ГОСТ 28147-89» (Магма) с длиной блока 64 бит. Эти алгоритмы были тщательно изучены соответствующими российскими организациями (правоохранительными органами и др.), были одобрены и приняты в качестве стандарта.

С января 2000 года проводился 40-месячный европейский криптографический проект NESSIE Европейский криптопроект. Данный проект является научно-исследовательским проектом в рамках Общества информационных технологий Программы Европейской Комиссии (IST), целью которого является отбор новых европейских криптостандартов на основе открытого конкурса (тендера). В результате отбора в качестве победителей был выбран ряд алгоритмов, таких как Camellia, MYSTY, SHACAL и AES.

Процесс применения современных методов криптоанализа для блочно-симметричных алгоритмов шифрования реализовывается на основе информации, полученной криптоаналитиком. Соответственно криптоанализ делится на следующие основные типы: 1) Анализ шифртекста для получения информации о ключе и алгоритме шифрования. 2) Анализ шифртекстов для

получения информации о ключе. 3) Анализ с открытым текстом для получения информации о ключе. 5) Анализ выбранных шифртекстов с целью получения информации о ключе. 6) Анализ с помощью выбранных текстов для получения информации о ключе. 7) Анализ с помощью выбранных ключей для получения информации о ключе.

В отношении алгоритмов блочно-симметричного шифрования имеются следующие современные методы криптоанализа, основанные на упомянутых выше типах криптоанализа: линейный, дифференциальный, линейно-дифференциальный, интегральный, алгебраический и другие.

Существуют следующие общие криптографические требования на преобразования алгоритмов блочно-симметричного шифрования:

1. Регулярность преобразований подстановки (S-блок);
2. Высокая степень алгебраической нелинейности булевой функции ($f_i(x)$), отражающие выходные биты S-блока;
3. Высокая степень корреляционной иммунности (*CI*) булевой функции $f_i(x)$;
4. Высокая лавинная эффективность (SAC) и принцип распространения булевой функции $f_i(x)$;
5. Высокий уровень значения нелинейности функции $f_i(x)$
6. Высокий уровень значения нелинейности S-блока;
7. Высокий уровень значения алгебраического иммунитета S-блока;
8. Приближение к нулю значения *BIC* (принцип независимости битов) для S-блока.

Каждое из этих перечисленных требований служит основой для корректной работы алгоритма шифрования и, что наиболее важно, для обеспечения устойчивости на тот или иной метод криптоанализа. В частности, высокое значение нелинейности S-блока служит основанием для обеспечения стойкости к линейное криптоанализа, высокий алгебраический иммунитет для обеспечения стойкости к алгебраическому криптоанализу, регулярности, корреляционного иммунитета, лавинной эффективности и реализация принципов распространения служит основой для обеспечения стойкости к различным статистическим методам криптоанализа.

Во второй главе диссертации **«Исследование оценки стойкости алгоритма ГОСТ 28147-89 с использованием методов линейно-дифференциального и алгебраического криптоанализа»** приведены задачи по оценке алгоритма ГОСТ 28147-89 с использованием линейно-дифференциального (ЛДК) и алгебраического методов криптоанализа и их решения, полученные результаты и оценки.

Основная сущность метода ЛДК заключается в обобщении методов линейного (ЛК) и дифференциального (ДК) криптоанализа. Для оценки алгоритма ГОСТ 28147-89 необходимо решить следующие задачи:

1) Распределение количества раундов на методы ДК и ЛК;

2) Составление необходимых уравнений аппроксимации;

3) Определение значения разности высокого уровня эффективности;

4) Определение вариантов значения ключа последнего раунда.

Распределения – определяется количеством раундов алгоритма шифрования и эффективностью методов ДК и ЛК. Обозначим данное распределение как *Taqsimot([NДК], [NЧК]),* где: *Taqsimot*() – функция распределения, *NДК (NДК=$n_1,n_2,n_3,\ldots$. $n_i \in N$)* – применяемое количество раундов в методе ДК, *NЧК (NЧК=$n_1,n_2,n_3,\ldots$. $n_i \in N$)* – количество раундов, используемых в методе ЛК, *len(NДК)* – общее количество раундов, используемых методами ДК (ЛК), *[-]* – указывает на не использования ДК (ЛК). Следующее верно для данной функции.

Утверждение 1. Для алгоритма ГОСТ 28147-89 с количеством раундов *R (R>2),* уместно уравнение - *len[NДК]+len[NЧК]+2=R*.

Утверждение 2. Общее количество раундов, использованных при оценке алгоритма ГОСТ 28147-89 с использованием метода ЛДК, не превышает 4, т. е. уместно - *len*[*NЧК*]≤3.

В Таблице 1 приведены уравнения аппроксимации с высоким отклонением, которые обеспечивают возможность обнаружения частичных ключей, использованных в последнем раунде алгоритма, с использованием метода ЛК на раунды *len*(*NЧК*)≤*3* и их взаимосвязь с частичным ключом.

Таблица 1.

Необходимые уравнений аппроксимации

Ключ	*S* блок	Уравнение аппроксимации	Отклонение (*Δ*)	Вероятность (*p*)
K_1	S_7	$\Delta X_{25} \oplus \Delta Y_{17}=0$	*Δ=3/4*	*P=1/8*
K_2	S_7	$\Delta X_{28} \oplus \Delta Y_{14}=0$	*Δ=1/2*	*P=3/4*
K_3	S_1	$\Delta X_1 \oplus \Delta Y_{25}=0$	*Δ=1/2*	*P=3/4*
K_4	S_1	$\Delta X_4 \oplus \Delta Y_{24}=0$	*Δ=1/2*	*P=3/4*
K_5	S_2	$\Delta X_8 \oplus \Delta Y_{29}=0$	*Δ=1/2*	*P=3/4*
K_6	S_3	$\Delta X_{10} \oplus \Delta Y_{31}=0$	*Δ=1/2*	*P=1/4*
K_7	S_4	$\Delta X_{14} \oplus \Delta Y_3=0$	*Δ=1/2*	*P=1/4*
K_8	S_5	$\Delta X_{18} \oplus \Delta Y_7 \oplus \Delta Y_9=0$	*Δ=1/2*	*P=1/4*

Определение значения *разности высокого уровня эффективности* определяется количеством раундов и зависимостью раундов преобразований со свойствами распределения битов. Доказана следующая теорема:

Теорема 1. Пусть *M* ($M=m_1||m_2||m_3||\ldots||m_{64}$) – 64 битный открытый текст, *C* ($C=c_1||c_2||c_3||\ldots||c_{64}$) – 64 битный шифртекст, образованный в результате шифрования открытого текста *M* при помощи 256 битного *K* ($K=k_1||k_2||k_3||\ldots||k_{256}$) ключа посредством алгоритма ГОСТ 28147-89 с числом раундов *r* ($r \in \{1,2,3,\ldots 32\}$), а *w* – количество битов открытого текста, воздействующее на изменение значения какого-либо c_i ($i \in \{1,2,3,\ldots 64\}$). Если $r \geq 8$, то для c_i в любом значении *i* имеет место равенство *w*=64.

По результатам оценки алгоритма ГОСТ 28147-89 при помощи ЛДК метода, имеют место следующие.

Утверждение 3. Общее число раундов с применением ДК метода в процессе оценки алгоритма ГОСТ 28147-89 при помощи ЛДК метода не превышает 9, т.е. имеет место *len*[*NДК*]≤9.

Утверждение 4. Алгоритм ГОСТ 28147-89 с числом раундов 12 и более практически стойкий к ЛДК методу.

Выражение алгоритма через систему уравнений при применении метода алгебраического криптоанализа к алгоритму шифрования ГОСТ 2814789 требует решения следующих задач:

a) декомпозиция алгоритма шифрования;

b) алгебраическое выражение каждого элемента;

c) связать вход и выход каждого элемента с другими элементами, а также с ключом, открытым текстом и битами шифртекста;

Алгоритм, разработанный для построения системы уравнений со степенью $deg \leq 2$, выражающий S-блоки алгоритма ГОСТ 2814789 ($n=4$):

1. *Сформировать проверочную таблицу для отображения S блока.*
2. *Построить АНФ в отношении каждых исходящих $f_1, f_2, \ldots, f_k$ $(k=(3n^2+n)/2)$ функций проверочной таблицы.*
3. *Если выполняется $2n^2+n+1>2^n$, «сформировать линейные свободные уравнения в количестве m $(2n^2+n-2^n+1 \leq m \leq k)$ с выполнением условия $deg \leq 2$, используя соответствующие комбинации всех АНФ», в обратном случае закончить.*
4. *Объявить в качестве результативных уравнений все уравнения, где $deg \leq 2$ и закончить.*

Для преобразования сложения раундовых ключей ($z=F(x,k)$) использованных в алгоритме шифрования имеют место следующие утверждения:

Утверждение 5. Для каждой исходящей z_i-функции отображения $z=F(x,k)$ верно равенство $\deg(z_i)=i$.

Утверждение 6. В отношении отображения $z=F(x,k)$ верны следующие $z_i=x_i \oplus k_i \oplus k_{i-1}$, $z_i=x_i \oplus x_{i-1} \oplus k_i$ $(2 \leq i \leq 32)$ уравнения, выполняемые с вероятностью $p=0{,}75$ и наиболее эффективны для криптоанализа.

Согласно результатам оценки алгоритма ГОСТ 28147-89 при помощи метода алгебраического криптоанализа имеет место утверждение:

Утверждение 7. Алгоритм ГОСТ 28147-89 с числом раундов 5 и более практически стойкий к методу алгебраического криптоанализа.

В третьей главе **«Создание алгоритма блочного симметричного шифрования»** приведены процессы разработки алгоритма блочного симметричного шифрования, на основе SP сети, его криптографических преобразований и генерации раундовых ключей.

При разработке преобразований новых алгоритмов шифрования на основании SP-сети базировалось на принципы простоты и быстродействий, имеющие свойства «рассеивание» и «перемешивание», а также удовлетворяющие общие криптографические требования, устойчивые к современным методам криптоанализа и с высокими криптографическими показателями.

В качестве основного нелинейного отображения, обеспечивающего свойство перемешивания, разработаны 2 S-блока (8x8)-размера. Криптографические показатели данных S-блоков приведены в таблицах 2 и 3.

Таблица 2.

Криптографические показатели S_1(8x8)-блока

Показатели	**S_1(8x8)-блок**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
сбалансированности	+	+	+	+	+	+	+	+
регулярности	+							
deg(*f*)	7	7	7	7	7	7	7	7
N(*f*)	112	112	112	112	112	112	112	112
N(*S*)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	8	8	4	6	8	8	8	6
Δ	4							
D(*S*)	878220							
Слабая точка	–							
AI(S)	2							

S_1(8x8)-блок обеспечивает повышение стойкости алгоритма шифрования к линейным, дифференциальным, линейно-дифференциальным методам криптоанализа. Данный S-блок был создан при помощи конструкции Ниберг, на основе критериев повышенности *D*(*S*) параметра и отсутствия слабой точки.

Таблица 3.

Криптографические показатели S_2(8x8)-блока

Показатели	**S_2(8x8)-блок**							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
сбалансированности	+	+	+	+	+	+	+	+
регулярности	+							
deg(*f*)	7	7	7	7	7	7	7	7
N(*f*)	106	108	108	108	106	110	106	106
N(*S*)	104							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	8	10	6	8	8	8	12	8
Δ	8							
D(*S*)	31050							
Слабая точка	–							
AI(S)	3							

S_2(8x8)-блок обеспечивает повышение стойкости алгоритма шифрования к алгебраическим и другим методам криптоанализа.

Алгоритм разработки данного S-блока был создан следующим образом (для $S(8x8)_{max}$ – блока верно $N(S)$=112):

1. $S(8x8)=S(8x8)_{max}$.
2. *Взаимозаменить случайные 39 элементов S(8x8)-блока*

3. *Определить значения N(S) и δ параметров S(8x8)-блока, образованного в результате 2-шага.*
4. *Если N(S)<104 или δ>8 перейти к 1-шагу.*
5. *Определить значения AI(S) и N_{TS} параметров S(8x8)-блока, образованного в результате 2-шага.*
6. *Если AI(S)≠3 или N_{TS}≠441 перейти к 1-шагу.*
7. *Объявить S(8x8)-блок как исходящие данные и закончить.*

В качестве основного отображения, обеспечивающего свойство рассеивания, было использовано действие умножения нижеприведённой матрицы *MDS* (Maximum Distance Separable) (8x8)-порядка к матрице (8x*w*)-порядка в конечной поле $GF(2^8)/\varphi(x)$ ($\varphi(x)=x^8\oplus x^7\oplus x^6\oplus x\oplus 1$).

$$MDS=\begin{bmatrix}1,2,3,4,5,112,145,225\\2,1,4,3,112,5,225,145\\3,4,1,2,145,225,5,112\\4,3,2,1,225,145,112,5\\5,112,145,225,1,2,3,4\\112,5,225,145,2,1,4,3\\145,225,5,112,3,4,1,2\\225,145,112,5,4,3,2,1\end{bmatrix}$$

Утверждение 8. Данная матрица инволютивна и скоростная (легкая) матрица.

Ключи раунда прибавляются (вычитываются) по модулю 2^n ($16\le n\le 64$), и данным действием повышают стойкость алгоритма шифрования к интегральному методу криптоанализа и большинства.

Алгоритм шифрования, позволяя зашифровать и расшифровать блок данных длиной в 128, 256, 384 и 512 бит при помощи соответственно 8, 10, 12, 14 раундов, может использовать секретный ключ, длина которого превышает длину блока и состоит из 128, 256, 384 и 512 бит.

В общем случае, для алгоритма с "*r*" раундом имеют место следующие формулы зашифрования и расшифрования:

$$C=K(...K(S(T(B(K(S(T(B(K(M,Rk_0)))),Rk_1))))),Rk_2)...,Rk_r);$$

$$M=K^{-1}(...K^{-1}(B^{-1}(T(S^{-1}(K^{-1}(B^{-1}(T(S^{-1}(K^{-1}(M,Rk_r))))),Rk_{r-1}))))),Rk_{r-2})...,Rk_0)$$

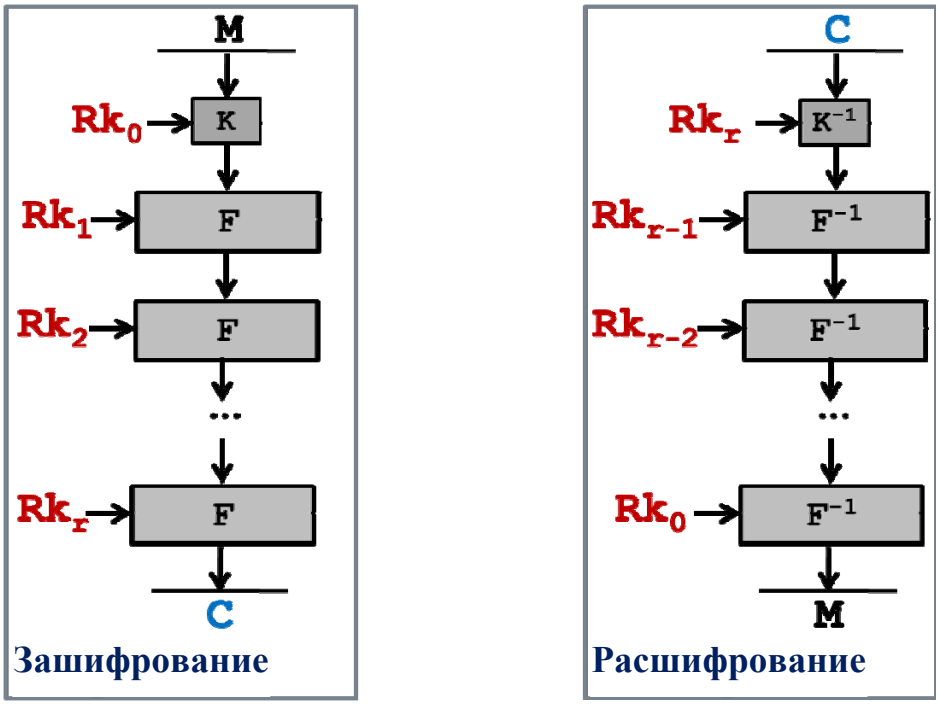
Утверждение 9. Используя *B*, *T*, *S*, *K* отображения достигается максимальной лавинной эффективности после 2-раунда.

При разработке функции генерации раундовых ключей основывались на выполнение следующих требований:

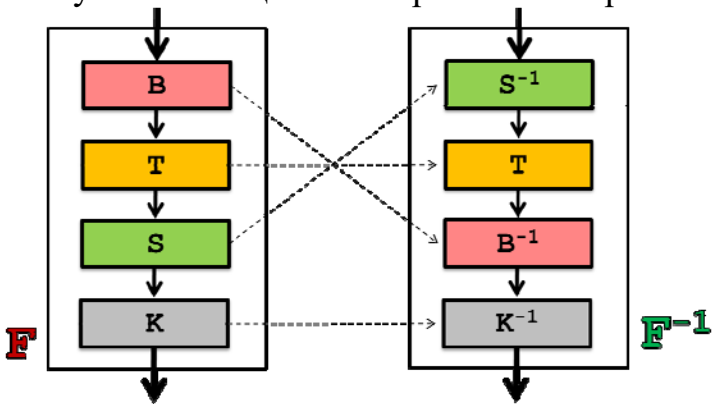
- односторонность (необратимость);
- адаптированность к входящим и исходящим значениям разной длины.

Для функции (φ) генераций ключей раунда на основе секретного ключа имеет место следующая теорема.

Теорема 2. Если *key* – секретный ключ, а Rk_i – ключ раунда *i* ($i\ge 0$), то верно следующее выражение: $Rk_i = \varphi(key, i)$



Рисунка 1. Общая схема работы алгоритма



Рисунка 2. Общая схема работы функция раунда

В четвертой главе диссертации **«Оценка криптостойкости созданного блочного симметричного алгоритма шифрования»** дается оценка стойкости созданного алгоритма шифрования и различных криптографических показателей.

Экспериментально найденные оптимальные разности для применения дифференциального метода криптоанализа к созданному алгоритму шифрования приведены в таблице 4.

Таблица 4.

Найденные оптимальные разности для 128 битного блока

После *r*-раунда	**Количество необходимых текстов**	**Варианты разности** (в шестнадцатеричной системе счислении)
3	2^{127}	00000000002300660000000000000000
4	2^{219}	0000002D000000000000000000000C0
5	2^{303}	00000000000000EC00000000000000EC
6	2^{393}	0000000000000000EF00270000000000
7	2^{479}	00000000000000C000000000000000EC
8	2^{570}	00000000000000EC00000000000000C0

По результатам оценки стойкости алгоритма шифрования дифференциальным методом криптоанализа было определено, что в общем случае, число текстов, требующихся для криптоанализа алгоритма с длиной блока в l бит, может увеличиваться после каждого раунда на $\approx 2^{91 \bullet \frac{l}{128}}$.

Утверждение 10. Созданный алгоритм является практически устойчивым к дифференциальному методу криптоанализа после 4-раунда.

К уравнениям, сформированным для применения линейного метода криптоанализа к алгоритму, имеет место, следующее:

Количество линейных уравнений с предельным отклонением в отношении $S_1(8,8)$-блока составляет 255, значение отклонения которых равно 0,125.

Количество линейных уравнений с предельным отклонением в отношении $S_2(8,8)$-блока составляет 33, значение отклонения которых равно 0,1875.

Для битов, входящих в отображение умножения на MDS матрицу (x_0, x_1, x_2,…, x_{63}) и выходящих из него битов (y_0, y_1, y_2,…, y_7) верно следующее типовое уравнение, выполняемое с вероятностью p=1:

$$y_0=x_0 \oplus x_8 \oplus x_9 \oplus x_{17} \oplus x_{25} \oplus x_{26} \oplus x_{32} \oplus x_{33} \oplus x_{34} \oplus x_{46} \oplus x_{54} \oplus x_{55} \oplus x_{56}$$

Утверждение 11. Созданный алгоритм стойкий к линейному методу криптоанализа после 3-раунда.

Согласно результатам оценки на алгебраический метод криптоанализа имеет место следующее утверждение.

Утверждение 12. Созданный алгоритм практически стойкий к алгебраическому методу криптоанализа после 3-раунда.

ЗАКЛЮЧЕНИЕ

Диссертационная работа посвящена оценке стойкости алгоритма ГОСТ 28147-89 линейно-дифференциальным и алгебраическим методами криптоанализа и созданию блочного симметричного алгоритма шифрования с высокой стойкостью.

Основные результаты исследования заключаются в следующем:

1. Применены линейно-дифференциальный и алгебраический методы криптоанализа к алгоритму ГОСТ 28147-89 и оценена стойкость алгоритма.

2. Разработан метод описания криптографических преобразований при помощи алгебраических уравнений нижней степени.

3. Разработан алгоритм построения S-блока с максимальным алгебраическим иммунитетом и высокой степенью нелинейности.

4. Разработан новый алгоритм шифрования, основанный на SP-сети, с возможностью работы с различными длинами блоков и ключа.

5. Разработан алгоритм генерации раундовых ключей с использованием преобразований шифрования.

6. На основе дифференциального, линейного и алгебраического методов криптоанализа оценена стойкость вновь созданного алгоритма шифрования.

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

NATIONAL UNIVERSITY OF UZBEKISTAN

SATTAROV ALIJON BOZORBOYEVICH

EVALUATION OF STABILITY OF THE ALGORITHM GOST 28147-89 BY LINEAR-DIFFERENTIAL AND ALGEBRAIC CRYPTANALYSIS METHODS AND DEVELOPMENT CIPHER WITH HIGHER STABILITY

05.01.05 – Methods and systems of information protection. Information security

ABSTRACT OF DISSERTATION OF THE DOCTOR OF PHILOSOPHY (PhD) ON PHYSICAL AND MATHEMATICAL SCIENCES

TASHKENT-2019

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2018.1.PhD/FM190.

Dissertation has been prepared at National University of Uzbekistan.

The abstract of the dissertation is posted in three languages (uzbek, russian, english (resume)) on the website (www.ik-fizmat.nuu.uz) and the "ZiyoNet" Information and educational portal (www.ziyonet.uz).

Scientific supervisor:	**Abdurakhimov Bakhtiyor Fayzievich** Doctor of Physical and Mathematical Sciences, Professor
Official opponents:	**Tuychiev Gulom Numonovich** Doctor of Physical and Mathematical Sciences
	Xudoykulov Zarif Turakulovich Doctor of philosophy on technical sciences
Leading organization:	**SUE «UNICON.UZ»**

Defense will take place «____» _____2019 at _____ at the meeting of Scientific Council number DSc.27.06.2017.FM.01.02 at National University of Uzbekistan. (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 227-12-24, fax: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

Dissertation is possible to review in Information-resource centre at National University of Uzbekistan (is registered №____) (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 246-02-24).

Abstract of dissertation sent out on «____» _____2019 year

(Mailing report № _____on «____» _____2019 year)

A.R.Marakhimov
Chairman of Scientific council
on award of scientific degrees,
D.F.-M.S., professor

Z.R.Rakhmonov
Scientific secretary of Scientific
council on award of
scientific degrees, D.F.-M.S.

R.D.Aloyev
Chairman of Scientific seminar
under scientific council on award
of scientific degrees,
D.F.-M.S., professor

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is evaluation of stability of the encryption algorithm GOST 28147-89 by linear-differential and algebraic cryptanalysis methods and of development block-symmetric encryption algorithm with higher cryptographic stability.

The object of the research work are encryption algorithm of GOST 28147-89, linear-differential and algebraic cryptanalysis, methods for constructing cryptographic transformations for block-symmetric encryption algorithms and object-oriented software.

Scientific novelty of research work is as follows:

developed the method for describing cryptographical operations using low degree algebraic equations;

developed the block-symmetric encryption algorithm, based on the SP network and evaluated its stability;

developed the algorithm for constructing an 8x8 S-block with a maximum algebraic immunity and a high degree of nonlinearity, based on the permutation;

developed the most fast and involutory MDS matrix, 8x8 in size, defined over a finite field;

developed the software of new high-stability block-symmetric encryption algorithm, based on the SP network.

Implementation of the research results. Scientific results in the evaluation of the stability of the algorithm GOST 28147-89 by linear-differential and algebraic methods of cryptanalysis and the development of a cipher with higher cryptographic stability are introduced, into practice in the following areas:

the algorithm for the development of S-boxes tables was applied to the generation of the S-boxes in the software “Zebra” used in the Ministry of Defense of the Republic of Uzbekistan (Reference No. 20/2061 of April 8, 2019, the Center of radioelectronic systems and information technologies). The results of research allowed in a short time to generate stability tables of S-boxes of an arbitrary finite number;

the algorithm for the development of S-boxes tables was applied to the generation of the S-boxes in the software “Generator” used in the Ministry of Defense of the Republic of Uzbekistan (Reference No. 20/2061 of April 8, 2019, the Center of radioelectronic systems and information technologies). The results of research allowed in a short time to generate stability tables of exchange by size 8x8.

The structure and volume of the thesis: The thesis consists of an introduction, four chapters, conclusion, a list of used literature and 16 applications. The volume of the thesis is 110 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (1 часть; part 1)

1. Sattarov A.B. About the algorithm of data encryption BTS // International Journal of Advances in Computer Science and Technology, 7(6), 2018, 36-39. (5. Global Impact Factor. IF=0.499).
2. Abduraximov B.F., Sattarov A.B. S-blokni ifodalovchi algebraik tenglamalar sistemasini qurish algoritmi // Проблемы вычислительной и прикладной математики, №2(14), 2018, 132-145. (01.00.00; №9)
3. Sattarov A.B. Bul funksiyaning algebraik immunitetini aniqlash algoritmi // Информатика ва энергетика муаммолари, №3, 2018, 30-38. (05.00.00; №5)
4. Саттаров А.Б. ГОСТ 28147-89 стандарт шифрлаш алгоритми криптобардошлиги ҳақида // Ахборотkоммуникациялар: Тармоқлар, Технологиялар, Ечимлар, №3 (47), 2018, 52-58. (05.00.00; №2)
5. Sattarov A.B. Constructing S-Boxes for Block Symmetric Encryption // Saudi Journal of Engineering and Technology, 4(3), 2019, 123-126. (41. SCImago. IF=0.172).

II бўлим (2 часть; part 2)

6. Abdurakhimov B.F., Sattarov A.B. An algorithm for constructing S-boxes for block symmetric encryption // International Journal: “Universal Journal of Mathematics and Applications”. 1 (1) (2018) 29-32.
7. Abdurakhimov B.F., Sattarov A.B. S-box development method based on the Boolean function // Abstracts of the International conference “Modern problems of applied mathematics and information technologies - al-Khorezmi 2018” (September 13-15, 2018) - Tashkent, NUUz named after Mirzo Ulugbek, 2018 –pp.68-69.
8. Sattarov A.B. Algebraik bardoshli S-bloklarni qurish algoritmi // «Актуальные проблемы прикладной математики и информационных технологий – Аль-Хорезми 2016»: Труды международной конференции (9-10 ноября 2016 г. БухГУ). Бухара. 2016. –с.130-132.
9. Абдурахимов Б.Ф., Саттаров А.Б. Об алгоритме шифрование данных БТС // “Davlat boshqaruvi va ta`lim tizimida axborot-kommunikatsiya texnologiyalarini qo‘llashdagi muammolar va yechimlar”: ilmiy-amaliy konferensiya materiallari to‘plami. – T.: TDYU, 2017. – 338-342 bet.
10. Абдурахимов Б.Ф., Саттаров А.Б. Способ построения S-блоков повышенной криптостойкости // “Davlat boshqaruvi va ta’lim tizimida axborot-kommunikatsiya texnologiyalarini qo`llashdagi muammolar va yechimlar”: ilmiy-amaliy konferensiya materiallari to‘plami. – T.: TDYU, 2017. – 342-344 bet.
11. Абдурахимов Б.Ф., Саттаров А.Б. Шифрлаш алгоритмлари учун максимал тарқатиш хусусиятига эга бўлган акслантиришларни ишлаб чиқиш //

"Contemporary Problems in Mathematics and Physics": Abstracts of the Uzbek-Israel International Conference (October 6–10, 2017, Tashkent). – Tashkent. 2017. –pp.129-132.
12. Курьязов Д.М., Саттаров А.Б. Вопросы выбора оптимальных разностей при применении линейно-дифференциального метода криптоанализа // «Информационная безопасность в свете Стратегии Казахстан-2050»: Сборник трудов I Международной научно–практической конференции (12 сентября 2013 г., Астана). – Астана. 2013. –с.386–391.
13. Курьязов Д.М., Саттаров А.Б. Метод построения алгебраической системы уравнений, описывающей S – блок // «Информационная безопасность в свете Стратегии Казахстан-2050»: Сборник трудов III Международной научно–практической конференции (15-16 октября 2015 г., Астана). – Астана. 2015. –с.222–229.
14. Саттаров А.Б. Буль функциянинг алгебраик иммунитетини аниқлаш алгоритми // «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения»: Сборник тезисов республиканской семинара (28 октября 2015 г. Мининфокомом). – Ташкент. 2015. –с.49-51.
15. Саттаров А.Б. Чизиқли-дифференциал криптотаҳлил усулининг ГОСТ 28147-89 алгоритмига қўллаш масаласи // «Прикладная математика и информационная безопасность»: Материалы республиканской конференции (28-30 апреля 2014 г. НУУз). –Ташкент. 2014. –с.361-366.
16. Саттаров А.Б. Шифрлаш алгоритмлари криптобардошлигини баҳолашда алгебраик криптотаҳлил усулининг қўлланиш асослари // «Актуальные проблемы прикладной математики и информационных технологий – Аль-Хорезми 2014»: Труды международной конференции (15-17 сентября 2014 г. НУУз). –Ташкент. 2014. –с.47–51.
17. Саттаров А.Б. Шифрлаш алгоритмлари криптобардошлигини баҳолашда чизиқли-дифференциал криптотаҳлил усулининг қўлланиш асослари // «Информационные технологии и проблемы телекоммуникаций»: Сборник докладов республиканской конференции (14-15 марта 2013 г. ТУИТ). – Ташкент. 2013. –с.251-252.

Автореферат Ўзбекистон Миллий университетининг «ЎзМУ хабарлари»
журнали таҳририятида 2019 йил 1 июнда таҳрирдан ўтказилди.

Бичими 60x84$^{1}/_{16}$.Рақамли босма усули. Times гарнитураси.
Шартли босма табоғи:2,5. Адади 100. Буюртма № 65.

Гувохнома reestr № 10-3719
«Тошкент кимё технология институти» босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Навоий кўчаси, 32-уй.