ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.03/30.12.2019.FM.01.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

БОЙҚУЗИЕВ ИЛХОМ МАРДАНОҚУЛОВИЧ

КРИПТОТАҲЛИЛ УСУЛЛАРИНИНГ КУЗНЕЧИК ШИФРЛАШ АЛГОРИТМИГА НИСБАТАН ҚЎЛЛАНИЛИШИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

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

Тошкент-2022

УДК: 004.056.55

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

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

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

Бойқузиев Илхом Марданокулович
Криптотаҳлил усулларининг Кузнечик шифрлаш алгоритмига нисбатан қўлланилиши …….....3

Бойқузиев Илхом Марданокулович
Применение методов криптоанализа к алгоритму шифрования Кузнечик 21

Boykuziev Ilkhom Mardanokulovich
Application of cryptanalysis methods to Kuznyechik encryption algorithm 41

Эълон қилинган ишлар рўйхати
Список опубликованных работ
List of published works 45

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.03/30.12.2019.FM.01.02 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

БОЙҚУЗИЕВ ИЛХОМ МАРДАНОҚУЛОВИЧ

КРИПТОТАҲЛИЛ УСУЛЛАРИНИНГ КУЗНЕЧИК ШИФРЛАШ АЛГОРИТМИГА НИСБАТАН ҚЎЛЛАНИЛИШИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

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

Тошкент-2022

Физика-математика фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида **B2022.1.PhD/FM618 рақам билан рўйхатга олинган.**

Диссертация Ўзбекистон миллий университетида бажарилган.

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

Илмий раҳбар:	**Абдурахимов Бахтиёр Файзиевич** физика-математика фанлари доктори, профессор
Расмий оппонентлар:	**Тўйчиев Ғулом Нўмонович** физика-математика фанлари доктори
	Курьязов Давлатёр Матякубович физика-математика фанлари доктори
Етакчи ташкилот:	**«UNICON.UZ» ДУК - Фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Ўзбекистон миллий университети ҳузуридаги илмий даражалар берувчи DSc.03/30.12.2019.FM.01.02 Илмий кенгашнинг 2022 йил «23» август соат 16 даги мажлисида бўлиб ўтади. (Манзил: 100174, Тошкент шаҳри, 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 университети Ахборот-ресурс марказида танишиш мумкин (98 рақам билан рўйхатга олинган). (Манзил: 100174, Тошкент шаҳри, Олмазор тумани, Университет кўчаси, 4-уй. Тел.: (99871) 246-02-24).

Диссертация автореферати 2022 йил «10» август да тарқатилди.
(2022 йил «13» июн даги 7 рақамли реестр баённомаси.)

М.М. Арипов
Илмий даражалар берувчи илмий кенгаш раиси, ф.-м.ф.д., профессор

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

Ғ.У. Жўраев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, ф.-м.ф.д., доцент

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳон миқёсида симметрик блокли шифрлаш алгоритмларини криптотаҳлиллаш муаммоларига, жумладан шифрлаш калитини аниқлашга қаратилган ва алгоритм таркибидаги акслантиришларнинг математик хусусиятларига, алгоритм қадамларига боғлиқ равишда, шунингдек математик хусусиятлар ҳамда қадамларга боғлиқ бўлмаган равишда ўтказиладиган крипто-ҳужумларни амалга ошириш масалаларига алоҳида аҳамият берилмоқда. Шифрлаш алгоритмларида фойдаланилган акслантиришларнинг хоссаларини ўрганиш, алгоритмларни мавжуд криптотаҳлил усулларига баҳолаш масалалари ахборот хавфсизлиги, амалий математика, криптография, криптотаҳлил ва объектга йўналтирилган дастурлаш каби соҳаларда олиб борилаётган илмий изланишларнинг тадқиқот объекти саналади. Шу сабабли, стандарт алгоритмларни криптотаҳлилнинг бардошлилик талаблари бўйича доимий таҳлил қилишга алоҳида эътибор қаратилмоқда.

Ҳозирги кунда жаҳонда ахборот хавфсизлиги дастурий ва аппарат-дастурий воситалар ёрдамида таъминланади, шу боис уларнинг криптомодулини ташкил қиладиган давлат миқёсида ёки давлатлараро миқёсда қабул қилинган стандарт криптографик алгоритмлар ва протоколлар кенг тадқиқ этилмоқда. Мазкур криптографик алгоритмлардан симметрик шифрлаш алгоритмлари ахборотларни сақлаш, қайта ишлаш, узатиш жараёнида махфийликни таъминлайди. Шунинг учун стандарт симметрик шифрлаш алгоритмларини таҳлил қилиш, уларни замонавий криптотаҳлил усулларига узлуксиз равишда баҳолаб бориш мақсадли илмий тадқиқотлардан ҳисобланади.

Мамлакатимизда фундаментал фанларнинг илмий ва амалий татбиқи сифатида ахборот хавфсизлиги, криптология соҳаларида бардошли криптографик алгоритмларни яратиш каби долзарб йўналишларга катта эътибор қаратилмоқда. Ахборотнинг махфийлигини ва бутунлигини таъминлашда симметрик блокли шифрлаш алгоритмларидан фойдаланишга, симметрик блокли шифрлаш алгоритмларини криптотаҳлил усулларига баҳолашга қаратилган усул ва алгоритмларни яратишга ҳамда қўллашга оид кўплаб илмий тадқиқотларда салмоқли натижаларга эришилди. «Алгебра ва функционал анализ, амалий математика ва математик моделлаштириш, ҳисоблаш математикаси ва дискрет математика, эҳтимоллар назарияси ва математик статистика»[1] фанларининг устувор йўналишлари бўйича халқаро стандартлар даражасидаги илмий изланишлар олиб бориш асосий вазифалар ва фаолият йўналишлари этиб белгиланган. Қарор ижросини таъминлашда стандарт шифрлаш алгоритмларини криптотаҳлил усулларига баҳолаш ҳамда олинган натижаларни амалиётга жорий қилиш муҳим аҳамиятга эга.

Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60 сонли “2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг

[1] Ўзбекистон Республикаси Президентининг 2020 йил 7 майдаги “Математика соҳасидаги таълим сифатини ошириш ва илмий- тадқиқотларни ривожлантириш чора-тадбирлари тўғрисида” ги ПҚ-4708-сон қарори.

тараққиёт стратегияси тўғрисида”ги, 2017 йил 7 февралдаги ПФ-4947 сонли “Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида”ги Фармонлари, 2007 йил 3 апрелдаги ПҚ-614-сон “Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисида”ги, 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 апелдаги ПҚ-2909-сон “Олий таълим тизимини янада ривожлантириш чора-тадбирлари тўғрисида”ги, 2018 йил 27 апрелдаги ПҚ-3682 “Инновацион ғоялар, технологиялар ва лойиҳаларни амалиётга жорий қилиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги Қарорлари, Ўзбекистон Республикаси Вазирлар маҳкамасининг 2007 йил 21 ноябрдаги 242-сон “Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги низомни тасдиқлаш ҳақида”ги қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий хужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти муайян даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Мазкур тадқиқот республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Муаммонинг ўрганилганлик даражаси. Симметрик блокли шифрлаш алгоритмларини криптотаҳлиллаш ва бардошли симметрик блокли шифрларни яратиш масалалари бўйича кўплаб олимлар илмий изланишлар олиб боришган. Жумладан, Б.Шнайер, Ю.Додис, Н.Фергюсон, Ж.Келси, М.Мацуи, Л.Кнудсен, Н.Куртуа, Н.Харрис, Э.Бихам, А.Шамир, Ж.Л.Масси, Р.Олейников, Е.Ищукова, Л.Бабенко, О.Казимировлар томонидан шифрлаш алгоритми ва бардошли криптографик акслантиришларни ишлаб чиқиш ҳамда уларни криптотаҳлил усулларига баҳолаш бўйича илмий-тадқиқотлар олиб борилган.

Мавжуд симметрик блокли шифрлаш алгоритмларини замонавий криптотаҳлил усуллари билан баҳолаш бир қанча олимлар томонидан тадқиқ қилинган. А.Жуков, Н.Молдовян, А.Молдовянлар томонидан ГОСТ 28147-89 алгоритми S-блоклари умумий криптографик талабларга, Л.Бабенко ва Е.Ищуковалар томонидан дифференциал криптотаҳлил усулига, Б.Абдурахимов ва А.Саттаровлар томонидан чизиқли дифференциал ва алгебраик криптотаҳлил усулларига, Р.Алоев ва Б.Ахмедовлар томонидан оддий ва такомиллашган слайдли таҳлил усулларига баҳоланган. М.Арипов ва Г.Туйчиевлар томонидан Лай-Месси тармоғи асосидаги симметрик блокли шифрлаш алгоритмлари чизиқли, дифференциал криптотаҳлил усулларига баҳоланган. П.Хасанов, М.Каримов, Х.Хасановлар томонидан параметрлар алгебраси асосида блокли симметрик шифрлаш алгоритми яратилган ва таҳлил қилинган. Б.Абдурахимов ва О.Аллановлар томонидан

O‘zDSt1105:2009 стандарт алгоритми алгебраик ва интеграл криптотаҳлил усулларига баҳоланган.

ГОСТ Р 34.12-2015 стандарти таркибидаги Кузнечик шифрлаш алгоритмининг замонавий криптотаҳлил усулларига баҳолаш ишлари қуйидаги олимлар илмий ишларида кўрилган, жумладан: Е.Толоманенко томонидан дифференциал таҳлил ўтказилиб, ундаги чизиқсиз S акслантириш ва чизиқли L акслантириш дифференциаллик хусусиятлари ўрнатилган; Е.Ищукова ва бошқалар томонидан Кузнечик алгоритмининг соддалаштирилган S-KN2 версияси учун чизиқли ва дифференциал криптотаҳлиллар олиб борилган; Г.Жураев ва бошқалар томонидан Кузнечик алгоритмининг 3 раунди учун дифференциал криптотаҳлилни амалга оширишнинг параллел алгоритми таклиф этилган; Е.Маро томонидан Кузнечик алгоритми учун алгебраик криптотаҳлил олиб борилган; А.Бирюков ва бошқалар томонидан мультитўпламли алгебраик криптотаҳлил усулига баҳоланган; R.AlTawy ва A.Youssef-лар томонидан “Ўртага учрашиш ҳужуми” усулига баҳолаш олиб борилган; В.Кирюкин томонидан калитга боғлиқ ҳолда амалга ошириладиган ҳужумларга баҳолаш бўйича илмий изланишлар олиб борилган. Интеграл криптотаҳлил усули ёрдамида шифрлаш алгоритмларини баҳолаш бўйича қуйидаги олимлар томонидан тадқиқотлар олиб борилган, жумладан: L.Knudsen томонидан Square шифрлаш алгоритмига нисбатан мазкур криптотаҳлил усули қўлланилган ва тегишли натижалар олинган; J.Daemen, L.Knudsen ва V.Rijmen лар томонидан AES шифрлаш алгоритми интеграл криптотаҳлил усулига баҳоланган; Y.Hu, Y.Zhang ва G.Xiao лар томонидан SAFER+ алгоритми интеграл криптотаҳлил усули ёрдамида баҳоланган; L.Knudsen ва D.Wagner-лар томонидан интеграл криптотаҳлил усулининг қўлланилиши бўйича илмий изланишлар олиб борилган.

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

Тадқиқотнинг мақсади Кузнечик симметрик шифрлаш алгоритмини бардошлигини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолашдан иборат.

Тадқиқотнинг вазифалари:

симметрик блокли шифрлаш алгоритмларини баҳолашда фойдаланиладиган криптотаҳлил усулларини таҳлил қилиш;

Кузнечик симметрик шифрлаш алгоритми ва ўқув алгоритмини алгебраик криптотаҳлил усули ёрдамида баҳолаш;

Кузнечик симметрик шифрлаш алгоритми ва ўқув алгоритмини интеграл криптотаҳлил усули ёрдамида баҳолаш;

уч раундли Кузнечик симметрик шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллашнинг самарали алгоритмини ишлаб чиқиш.

Тадқиқотнинг объекти сифатида симметрик шифрлаш алгоритми ҳамда криптотаҳлил жараёнлари олинган.

Тадқиқотнинг предметини Кузнечик симметрик шифрлаш алгоритми ҳамда унинг ўқув вариантини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш усуллари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида амалий криптография ва криптотаҳлил усуллари, сонлар назарияси, эҳтимоллар назарияси, қиёсий таққослаш ва объектга йўналтирилган дастурлаш воситалари ёрдамида тажрибалар ўтказиш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

Кузнечик симметрик шифрлаш алгоритмининг L акслантиришини ифодаловчи чизиқли тенгламалар ҳосил қилиш муаммоси чекли майдонда сонларни кўпайтиришни ифодаловчи тенгламалар ёрдамида ҳал қилинган;

Кузнечик симметрик шифрлаш алгоритмининг криптобардошлилиги алгебраик криптотаҳлил усули ёрдамида номаълумларнинг сонини камайтириш имконини берган тенгламаларни шифрлаш ва дешифрлаш йўналишида шакллантириш орқали баҳоланган;

Кузнечик симметрик шифрлаш алгоритмининг криптобардошлилиги интеграл криптотаҳлил усули ёрдамида бир байти актив бўлган очиқ матнлар тўпламидан фойдаланиб баҳоланган;

уч раундли Кузнечик симметрик шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллаб шифрлаш жараёнида фойдаланилган раунд калитларини аниқлаш алгоритми ишлаб чиқилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

Кузнечик шифрлаш алгоритми акслантиришларига тенгламалар шакллантириш имконини берувчи дастурий восита ишлаб чиқилган;

Кузнечик шифрлаш алгоритми акслантиришларини алгебраик ва интеграл криптотаҳлил усуллари ёрдамида баҳолаш имкониятини берувчи дастурий воситалар ишлаб чиқилган;

уч раундли Кузнечик шифрлаш алгоритми шифрлаш жараёнида фойдаланилган калитни интеграл криптотаҳлил усули ёрдамида топиш имконини берувчи дастурий восита ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Диссертацияда олинган натижаларнинг ишончлилиги унда математик мулоҳазаларнинг қатъийлиги, ўтказилган сонли тадқиқот натижалари билан тасдиқланганлиги ҳамда криптографик алгоритмларни криптотаҳлил усулларидан олинган реал ҳамда тажрибавий таҳлиллар билан асосланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти Кузнечик симметрик блокли шифрлаш алгоритмини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳоланганлиги билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти ўтказилган криптотаҳлил усуллари натижаларидан ва акслантиришларнинг криптографик характеристикаларидан замонавий шифрлаш алгоритмларини криптотаҳлил усуллари билан баҳолашда, янги шифрлаш алгоритмлари, янги акслантириш

функциялари ишлаб чиқишда асос сифатида ҳамда криптотаҳлил усулларини қўлланиши ўрганиш жараёнида фойдаланиш мумкинлиги билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Кузнечик шифрлаш алгоритмига алгебраик ва интеграл криптотаҳлили усулларининг қўлланилиши ва алгоритмнинг бардошлилигини баҳолашда олинган натижалар асосида:

диссертация ишининг илмий ва назарий маълумотларидан ҳамда криптографик алгоритмларнинг бардошлигини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш бўйича тавсиялардан, симметрик шифрлаш алгоритмининг акслантиришлари учун чизиқли тенгламаларни шакллантириш муаммоси ечими, алгебраик криптотаҳлилни амалга оширишда фойдаланилган ёндашув, алгебраик ва интеграл криптотаҳлил усулларини Кузнечик шифрлаш алгоритмига қўллаш ечимларидан «UNICON.UZ» ДУКда олиб борилаётган “Криптографик алгоритмлар яратиш” лойиҳасида криптотаҳлил усулларини таҳлил қилишда фойдаланилган («UNICON.UZ» ДУК - Фан-техника ва маркетинг тадқиқотлари марказининг 2022 йил 31 мартдаги 5-3/483-сонли маълумотномаси). Илмий натижаларнинг қўлланилиши «UNICON.UZ» ДУКда миллий ҳимояланган тизимларда фойдаланилаётган шифрлаш алгоритмлари бардошлигини баҳолаш, шифрлаш алгоритмини алгебраик ифодалашда номаълумлар сонини камайтириш, лойиҳа доирасида олиб борилаётган чизиқли ва алгебраик криптотаҳлил усулларини амалга ошириш жараёнида шифрлаш алгоритмларини ифодаловчи тенгламаларни шакллантириш имконини берган;

диссертация ишида олинган Кузнечик симметрик шифрлаш алгоритмининг ўқув варианти бардошлилигини криптотаҳлил усуллари ёрдамида баҳолаш ҳамда Кузнечик симметрик шифрлаш алгоритмининг бардошлилиги интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш натижаларидан ва Кузнечик симметрик шифрлаш алгоритмининг ўқув варианти бардошлилигини криптотаҳлил усуллари ёрдамида баҳолаш бўйича ёндашув Ф706-17-рақамли «Ахборот тизимларида биометрик – криптографик технологиялар қўлланилишининг тадқиқи» лойиҳасида маълумотларни криптографик ҳимоялаш алгоритмларини танлаш ва криптобардошлилигини баҳолашда фойдаланилган (Муҳаммад ал-Хоразмий номидаги ТАТУнинг 2022 йил 1 апрелдаги 968/15-01-сонли маълумотномаси). Илмий натижаларнинг қўлланилиши маълумотларни криптографик ҳимоялаш алгоритмларини танлаш ва криптобардошлилигини баҳолаш, симметрик блокли шифрлаш алгоритмлари акслантиришларининг интеграл ва алгебраик хусусиятларини аниқлаш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 3 та халқаро ва 3 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертация мавзуси бўйича жами 15 та илмий иш чоп этилган, жумладан, Ўзбекистон

Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш учун тавсия этилган илмий нашрларида 9 та мақола, шундан 6 таси хорижий ва 3 таси республика журналларида нашр этилган. Шунингдек, ЭҲМ учун яратилган 4 та дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 119 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети аниқланган, олинган натижаларнинг ишончлилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти, тадқиқот натижаларини амалда жорий этилиш ҳолати, нашр этилган ишлар ва диссертациянинг тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**ГОСТ Р 34.12.2015 шифрлаш стандарти алгоритмлари ва уларни криптотаҳлил усулларига баҳолаш натижалари**» деб номланган биринчи бобида симметрик блокли шифрлаш алгоритмларини баҳолашда фойдаланиладиган криптотаҳлил усуллари, ГОСТ Р 34.12.2015 шифрлаш стандарти алгоритмлари ва уларга нисбатан ўтказилган криптотаҳлил натижалари баён қилинган.

Криптотаҳлилчи K калитни бўлиши мумкин бўлган соҳасини камайтириш учун турли шароитларда шифрлаш калити тўғрисида қўшимча маълумот олишни мақсад қилади. Л.Кнудсен блокли шифрларни криптотаҳлиллаш усулларини олинган маълумот ҳажми ва сифатига кўра қуйидагича таснифлаган: *тўлиқ ҳужум*; *глобал дедукция*; *хусусий дедукция*; *ахборот дедукцияси*.

Ҳозирда симметрик блокли шифрларни таҳлиллашда кўплаб криптотаҳлил усулларидан фойдаланилиб, улар орасида қуйидагиларни алоҳида келтириш мумкин:

- дифференциал криптотаҳлил усули (differential cryptanalysis);
- чизиқли криптотаҳлил усули (linear cryptanalysis);
- чизиқли-дифференциал криптотаҳлил усули (linear-differential cryptanalysis);
- алгебраик криптотаҳлил усули (algebraic crypanalysis);
- интеграл криптотаҳлил усули (integral cryptanalysis).

Ушбу стандарт блок узунлиги $n = 128$ ва $n = 64$ бит ва калит узунлиги $k = 256$ бит бўлган иккита асосий блокли шифрни тавсифлайди. Ушбу стандартда тавсифланган блок узунлиги $n = 128$ бит бўлган шифрни «Кузнечик» («Kuznyechik») блокли шифри деб аталса, блок узунлиги $n = 64$ га тенг бўлган шифрни «Магма» («Magma») блокли шифри деб аташ мумкин.

Магма ва Кузнечик алгоритмларига нисбатан олиб борилган криптотаҳлил натижалари 1-жадвалда келтирилган.

1-жадвал

Замонавий симметрик шифрларнинг криптотаҳлил натижалари (D – танланган очиқ матн ёки шифрматнлар сони, M – хотира ҳажми ёки операциялар сони, T – сарфланган вақт, R- дешифрланган раундлар сони)

Шифрлаш алгоритми / Криптотаҳлил усуллари	**Магма**	**Кузнечик**
Чизиқли криптотаҳлил усули	- R=32, $T=2^{173,8}$ ва $D=2^{173,8}$. - 5-рауңддан сўнг тўлиқ бардошли бўлган.	- алгоритм мазкур таҳлил усулига тўлиқ бардошли деб топилган.
Дифференциал криптотаҳлил усули	- 6-рауңддан сўнг бардошли бўлган. - заиф S жадвал билан 32 раунд учун ҳужум бўлиш эҳтимоли 2^{-25} дан 2^{-33} гача бўлган.	- R=3 , $D= 2^{-108} + 6 * 2^{-120}$; - 3-рауңддан сўнг бардошли бўлиши исботланган; - алгоритм мазкур таҳлил усулига тўлиқ бардошли деб топилган.
Чизиқли-дифференциал криптотаҳлил усули	- 12-рауңддан сўнг бардошли бўлган.	-
Алгебраик криптотаҳлил усули	- R=3, M=45,43 Гбайт; - 5-рауңддан сўнг бардошли бўлган. - ҳужум мураккаблиги 2^{44} га тенг бўлган.	- $T=2^{154.5}$, $M=2^{140}$; - бир раунд учун усул мураккаблиги 2^{33} га тенг бўлган; - уч раундли SKN2 алгоритми учун XL усулида мантиқий тенгламаларни ечиш учун 236,33 секунд вақт ва 1,191 Гб тезкор хотира талаб қилинган.
Алгоритмларга нисбатан интеграл криптотаҳлиллаш амалга оширилмаган		
Бошқа ҳужум усуллари	- “Слайдли ҳужум” учун параллел дастурлаш алгоритми таклиф этилган.	- “Ўртада учрашиш” хужум усули: $D= 2^{113}$, $T=2^{140}$, $M=2^{153}$. - “Калитга боғлиқ” ҳужум: $T=2^{32}$, $M=2^{30}$, $D=2^{16}$.

Диссертациянинг **«Кузнечик шифрлаш алгоритмини алгебраик криптотаҳлил усули ёрдамида баҳолаш»** деб номланган иккинчи бобида Кузнечик шифрлаш алгоритмининг акслантиришларига нисбатан тенгламаларни шакллантириш, ўқув алгоритми S-KN1 ва Кузнечик шифрлаш алгоритмларига нисбатан алгебраик криптотаҳлил амалга оширилган.

Кузнечик шифрлаш алгоритмининг L акслантиришида кирувчи байтлар 148, 32, 133, 16, 194, 192, 251 сонларига кўпайтирилади ва бунинг учун тенгламалар тузиш қийинчилик туғдиради. Шу сабабли, ушбу кўпайтириш амалларини бўлакларга бўлиб амалга оширилса мақсадга мувофиқ бўлади. Яъни, мазкур сонларни 2, 4, 8, 16, 32, 64, 128 сонларининг йиғиндиси шаклида ифодалаш имконияти мавжуд. Шу сабабли, ушбу сонларга кўпайтириш амалини тенглама кўринишида ифодалаш орқали ушбу муаммони ечиш мумкин. Қуйида, шу мақсадда ҳосил қилинган тенгламалар ёрдамида 148 га кўпайтириш амали учун тузилган тенглама кўриниши келтирилган:

$$\mathbf{148}(x_7, x_6, x_5, x_4, x_5, x_6, x_7, x_0) mod\ p(x) = |128 + 16 + 4|$$
$$= x_5, x_4, x_5 + x_3, x_6 + x_4 + x_2 + x_0, x_5 + x_3 + x_1, x_4 + x_2 + x_1 + x_0, x_6 + x_3 + x_1, x_6 + x_2$$

Қолган 133, 194, 192, 251 сонларига кўпайтириш амаллари учун ҳам тенгламалар шу тартибда шакллантирилади:

148=128+16+4; 133=128+4+1; 194=128+64+2; 192=128+64; 251=128+64+32+16+8+2+1.

Юқорида келтирилган L акслантиришни ифодаловчи тенгламалардан алгебраик криптотаҳлил усулида фойдаланиш мумкин.

S-KN1 алгоритми учун ҳосил қилинган қисм элементларни алгебраик ифодалашда *X, S, L* – функцияларни кўриб ўтиш етарли. Тенгламаларнинг параметрларига таъсир кўрсатувчи акслантириш *S* акслантириши ҳисобланади.

***y=S(x)* - функция** –ўлчами 4x4 бит бўлган S акслантиришини амалга оширади (алмаштириш жадвали статик ҳисобланади).

Ушбу акслантиришга нисбатан тўғри (шифрлаш) йўналишда, тескари (матнни дастлабки ҳолатга ўгириш) йўналишда ва аралаш (даражаси пасайтирилган) алгебраик тенгламаларни қуриш мумкин, яъни:

1. $y_i = F(x_1, x_2, \dots, x_4)$, $i = 1,2, \dots ,8$
2. $x_i = F(y_1, y_2, \dots, y_4)$, $i = 1,2, \dots ,8$ **(1)**
3. $F(x_1, x_2, \dots, x_4, y_1, y_2, \dots, y_4) = 0$

S-KN1 шифрлаш алгоритми S акслантириши таҳлили умумий ҳолда қуйидаги жадвалда келтирилган:

2-жадвал

S-KN1 шифрлаш алгоритми S акслантиришининг криптографик кўрсаткичлари

Аргументлари	4	Регулярлик	+	N (φ)	0	AI(f)	1
Баланслашганлик	+	deg (f)	4	CI(f)	0	SAC(f)	-

S акслантириш учун **(1)** да келтирилган усулларда ҳосил қилинган тенгламалар параметрлари қуйидаги 3-жадвалда келтирилган.

Алгебраик криптотаҳлил усулининг кейинги босичида алгоритмнинг ҳар бир акслантириш учун ҳосил қилинган тенгламаларни боғлаб раунд учун тенгламаларни шакллантириш амалга оширилади.

3-жадвал

S-KN1 шифрлаш алгоритми S акслантиришига нисбатан тузилган тенгламалар параметрлари

	DEG	NS	4-даражали TS	3-даражали TS	2-даражали TS	1-даражали TS
1-усул	4	93	30	40	7	1
2-усул	4	93	30	48	-	-
3-усул	2	36	-	-	20	1

Акслантиришлар ўртасидаги боғланишларни **(1)** да келтирилган S акслантиришига нисбатан тенгламалар системасини тузиш усулларига боғлиқ равишда қуйидаги 3 хил усулда қуриш мумкин.

1. $y = L(S(X(x)))$ **(2)**
2. $x = X\left(S^{-1}\left(L^{-1}(y)\right)\right)$ **(3)**
3. $F\left(L\left(S\left(X(x)\right)\right), y\right) = 0$ **(4)**

Шундан сўнг раундларни ўзаро боғлаш жараёни амалга оширилади, яъни

улар асосида тўлиқ шифрлаш алгоритмини ифодаловчи умумий тенгламалар системаси шакллантирилади.

Кузнечик алгоритмининг раундларини боғлашни юқоридаги хусусиятларга мувофиқ, қуйидаги ёндашувлар ёрдамида амалга ошириш мумкин:

1. Ҳар бир раунд чиқишидаги массив битларини мустақил ифодаловчи тенгламаларни тузиш орқали.

$$y_i = R_i(x_i) = L\left(S\left(X(x_i)\right)\right),\ y_{i+1} = R_{i+1}(x_{i+1}) = L\left(S\left(X(x_{i+1})\right)\right) = L\left(S\left(X(y_i)\right)\right) = L\left(S\left(X\left(L\left(S(X(x_i))\right)\right)\right)\right) \quad \textbf{(5)}$$

2. Ҳар бир раунд киришидаги битларни ифодаловчи тенгламаларни тузиш орқали.

$$x_i = R^{-1}{}_i(y_i) = X\left(S^{-1}\left(L^{-1}((y_i))\right)\right),\ x_{i-1} = R^{-1}{}_{i-1}(y_{i-1}) = X\left(S^{-1}\left(L^{-1}((y_{i-1}))\right)\right) = X\left(S^{-1}\left(L^{-1}((x_i))\right)\right) = X\left(S^{-1}\left(L^{-1}\left(X\left(S^{-1}\left(L^{-1}((y_i))\right)\right)\right)\right)\right) \textbf{(6)}$$

3. Ҳар бир раунд киришида янги ўзгарувчи киритиш усули орқали.

$$F\left(L\left(A\left(X(x_{i+1})\right)\right), y_{i+1}\right) = F\left(S\left(A\left(X(y_i)\right)\right), y_{i+1}\right) = 0 \quad \textbf{(7)}$$

Раундларни боғлашни қуйидаги усуллар ёрдамида амалга ошириш мумкин:

1) **(2)** ифода ёрдамида шакллантирилган тенгламалар ёрдамида;
2) **(3)** ифода ёрдамида шакллантирилган тенгламалар ёрдамида;
3) дастлабки икки раундини **(2)** ва **(5)** ифодалар, учинчи раундини эса **(3)** ва **(6)** ифодалар ёрдамида шакллантирилган тенгламалар.

Қуйидаги 4-жадвалда юқорида келтирилган тенгламалар ёрдамида шакллантирилган уч раундли алгоритмни ифодаловчи тенгламалар системасининг номаълумлар сони келтирилган.

4-жадвал

Уч раундли алгоритмни ифодаловчи тенгламалар системасининг параметрлари

Раундларни боғлаш усули	**Номаълумлар сони**
1-усул	14232
2-усул	9320
3-усул	796

Кузнечик алгоритми учун ҳосил қилинган қисм элементларни алгебраик ифодалашда S – функция тенгламаларнинг параметрларига таъсир кўрсатувчи асосий акслантириш ҳисобланади.

***y=S(x)* - функция** – ўлчами 8x8 бит бўлган S акслантиришини амалга оширади. Ушбу акслантиришга нисбатан тўғри (шифрлаш) йўналишда, тескари (матнни дастлабки ҳолатга ўгириш) йўналишда ва аралаш (даражаси пасайтирилган) алгебраик тенгламаларни қуриш мумкин, яъни:

1. $y_i = F(x_0, x_1, \dots, x_7)$, $i = 0,1, \dots,7$
2. $x_i = F(y_0, y_1, \dots, y_7)$, $i = 0,1, \dots,7$ **(8)**
3. $F(x_0, x_1, \dots, x_7, y_0, y_1, \dots, y_7) = 0$

Кузнечик шифрлаш алгоритми S акслантириши таҳлили умумий ҳолда қуйидаги 5-жадвалда келтирилган:

5-жадвал

Кузнечик алгоритми S акслантиришининг криптографик кўрсаткичлари

Аргументлари	8	Регулярлик	+	N (f)	100	CI(f)	0	SAC(f)	-
Баланслашганлик	+	deg (f)	7	N (φ)	100	AI(f)	3		

S акслантириш учун **(8)** да келтирилган усулларда ҳосил қилинган тенгламалар параметрлари қуйидаги 6-жадвалда келтирилган.

6-жадвал

Кузнечик шифрлаш алгоритми S акслантиришига нисбатан тузилган тенгламалар параметрлари

	DEG	NS	7-даражали TS	6-даражали TS	5-даражали TS	3-даражали TS
1-усул	7	860	354	10	1	
2-усул	7	860	360	5	-	
3-усул	3	697	-	-	-	441

Кузнечик шифрлаш алгоритмида ҳам бир раунд учун ва раундларни боғловчи тенгламалар S-KN1 алгоритмида амалга оширилган усуллар ёрдамида шакллантирилади.

Раундларни боғлашни ўқув алгоритмида самарали ҳисобланган 3-усул ёрдамида шакллантирилган тенгламалар ёрдамида ифодаланганганда тенгламалар системасининг параметрлари қуйидаги 7-жадвалда келтирилган.

Саккиз раундли алгоритмни ифодаловчи системани сақлаш учун талаб қилинадиган хотира ҳажми эса 2^{62} ни ташкил қилади.

Диссертация ишининг «**Кузнечик шифрлаш алгоритмини интеграл криптотаҳлил усули ёрдамида баҳолаш**» номли учинчи боби S-KN1 ўқув алгоритмига нисбатан интеграл криптотаҳлилни амалга ошириш, S-KN1 ўқув алгоритмида фойдаланилган калитни аниқлашнинг самарали алгоритми ва Кузнечик ўқув алгоритмига нисбатан интеграл криптотаҳлилни амалга оширишга бағишланган.

7-жадвал

Алгоритмни ифодаловчи тенгламалар системасининг параметрлари

Раундлар сони	**Номаълумлар сони**	**Ҳотира ҳажми**	**Мураккаблик, ≈ O^3**
2 раунд	2^{17}	2^{25}	2^{51}
4 раунд	2^{28}	2^{35}	2^{72}
6 раунд	2^{41}	2^{48}	2^{123}
8 раунд	2^{55}	2^{62}	2^{165}

Интеграл криптотаҳлил усулини бирор-бир шифрлаш алгоритмига қўллаш учун, танлаб олинган очиқ матнлар ва уларга мос шифрматнларнинг махсус тўплами маълум бўлиши лозим. Очиқ матнлар тўпламини танлашнинг маълум қоидаларига кўра, S-KN1 шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллаш учун очиқ матнлар тўплами танланган ва кузатиш амалга оширилган.

Кузатиш жараёнидан, алгоритми биринчи раундида S акслантириш актив бўлакларни тарқатмаслиги, шунингдек, delta тўпламнинг баланслашганлигига таъсир қилмаслиги маълум бўлди. L акслантириши эса, устундаги битта актив бўлакни иккита актив бўлакларга тарқатади. X акслантириш ҳам баланслашганликга таъсир қилмайди, шунингдек, актив бўлакни тарқатмайди. Бу ерда, тўпламдаги актив бўлакларнинг сонига фақат

L акслантиришлари таъсир қилишини кўриш мумкин.

Худди шу тарзда, S-KN1 шифрлаш алгоритмининг кейинги раундлари учун ҳам тўпламнинг ўзгариши кузатиб борилади.

2-раунддан сўнг ҳам тўплам баланслашган бўлади. Кузатилаётгаи тўпламнинг шифрлаш алгоритми 3-раундидан кейинги ўзгариши қуйидаги 8- жадвалда келтирилган.

8 –жадвал

Кузатилаётган тўпламнинг 3-раунддан кейинги ўзгариши

Акс-ш	2-раунд сўнгидаги қиймат	3-раунд		
		S	L	X
1-блок	0011 0000	0111 0011	1010 1010	0011 0110
2-блок	0110 1110	0101 1101	0011 0010	1010 1110
3-блок	0011 0100	0111 1111	1101 0110	0100 1010
4-блок	0000 0100	0011 1111	1110 1010	0111 0110
5-блок	0010 1111	1010 1000	0101 0101	1100 1001
6-блок	0001 0111	0110 1011	0101 0001	1100 1101
7-блок	1110 1100	1101 0100	1101 0000	0100 1100
8-блок	1000 0100	0010 1111	1010 1001	0011 0101
9-блок	0100 0101	1111 0000	1001 0010	0000 1110
10-блок	1001 1100	1100 0100	1001 0011	0000 1111
11-блок	1000 1111	0010 1000	0011 1110	1010 0010
12-блок	1011 0111	1110 1011	0011 1010	1010 0110
13-блок	1011 1010	1110 0001	1110 0000	0111 1100
14-блок	0000 1010	0011 0001	1111 0100	0110 1000
15-блок	1001 1001	1100 1100	0010 1011	1011 0111
16-блок	1111 0110	1000 0101	1001 1110	0000 0010
(XOR)∑=	0000 0000	0011 1000	0111 1101	0111 1101

Қаралаётган шифрлаш алгоритмининг 3-раунд киришида кузатилаётган тўпламнинг баланслашган элементи мавжуд бўлиб, бу ҳолат шифрлаш алгоритмининг 4-раундда фойдаланилган раунд калитини аниқлаш имкониятини беради. Криптотаҳлилнинг 1-босқичини ушбу қадамда тўхтатиш мумкин. Криптотаҳлилнинг кейинги босқичи калит вариантларини аниқлаш бўлиб, ушбу жараёнда зарур ҳисобланган 3 –раунд сўнгидаги шифр матн тўплами ҳам маълум.

Криптотаҳлилнинг кейинги жараёни, яъни шифрлаш алгоритмининг сўнги раундида фойдаланилган калит қийматни аниқлаш, сўнги раундга кирувчи тўпламда актив (ёки пассив) байт мавжудлигини ҳамда сўнгги раунддан чиқувчи маълумот (шифр матн) ни билган ҳолда, статистика ўтказиш йўли орқали амалга оширилади.

Интеграл криптотаҳлил усули бўйича моҳиятига кўра 3 раундли S-KN1 алгоритмида сўнги раунд калити қийматни аниқлаш учун барча шифрматнлар тўпламини сўнгги раунд калитининг мумкин бўлган вариантларини тўлиқ танлаш усули билан бир раундга дешифрлаш амалга оширилиши зарур.

Ушбу қадамлар кетма-кетлигини бажариш жараёнида кўриш мумкинки, шифрматнлар тўпламини акслантиришдан ўтказиш жараёни калит вариантларини тўлиқ танлаш усулидан самарали эмас. Лекин, алгоритм акслантиришларининг хусусиятларидан фойдаланиб, самарали натижага

эришиш мумкин.

Алгоритмга интеграл криптотаҳлил усулини қўллаш ва калитни топишнинг самарали алгоритми таклиф этилди.

Уч раундли S-KN1 алгоритм учун интеграл криптотаҳлил усулида калитни топиш алгоритми қуйидагича:

1. Бир байти актив, қолган байтлари пассив очиқ матнлар тўплами танлаб олинсин;

2. Тўпламнинг барча массивлари учун 3 раундли шифрлаш амалга оширилсин;

3. Ҳосил бўлган шифр матнлар тўпламининг барча массивлари учун $a = L^{-1}(y)$ қийматлар ҳисоблансин;

4. k' ($k' = L^{-1}(k)$) нинг қабул қилиши мумкин бўлган барча вариантлари (0000 0000 дан 1111 1111 гача) ва x тўпламнинг барча $x_i = S^{-1}(a_i \oplus k'_i)$ ($i = 0,1$) элементлари учун $\sum x_i = 0$ тенглик текширилсин;

5. Тенгликни қаноатлантирадиган вариантлар танлаб олинсин ва k' нинг мос байти сифатида қабул қилинсин;

6. k' нинг ҳар бир байти ягона қиймат қабул қилмагунча, 1-5 қадамлар қайтарилсин ва ҳар сафар k' нинг бир байти учун қабул қилинган вариантлар билан аввал ҳосил қилинган вариантлар кесишмаси олинсин.

7. $L(k')$ ҳисоблансин ва учинчи раунд сўнгида фойдаланилган калит сифатида эълон қилинсин.

Мазкур алгоритмнинг учинчи раунд калитини топиш учун бажариладиган танлашлар сони ифода ёрдамида аниқланади: $n = a*b*c$

Бу ерда, a - шифрматн тўплами элементлари сони, b - шифр матнлар сони, c - актив ва пассив қисмлардан иборат танлаб олинган тўпламлар сони.

Ушбу таклиф этилган алгоритм асосида махсус дастурий таъминот яратилди, юқорида кўриб чиқилган мисолда қўлланилган калитни топиш жараёни амалга оширилди.

Дастурий таъминот ёрдамида олинган натижаларда k' нинг дастлабки ярим байти учун номзод сифатида қабул қилинган вариантлар тўрттани (**0011, 1001, 1101 ва 1111**), иккинчи ярим байт учун номзодлар эса иккитани (**0011 ва 1110**) ташкил қилди. Шу сабабли, номзод калитлар биттани ташкил қилмагунча 6-қадамда таъкидланганидек юқорида бажарилган кетма-кетликлар бошқа очиқ матнлар тўплами учун ҳам такрорланди.

Натижалардан маълум бўлдики k' нинг тастлабки ярим байти учун номзод сифатида қабул қилинган вариантлар иккитани (**0100 ва 1101**), иккинчи ярим байт учун номзодлар эса саккизтани (**0000, 0010, 0101, 0111, 1001, 1011, 1100 ва 1110**) ташкил қилди. Вариантларнинг кесишмаси олинганда k' нинг дастлабки ярим байти учун **1101**, иккинчи ярим байти учун эса **1110** қийматлар ҳосил бўлади. Демак, $k' = 11011110$ ва $k = L(k') = 10011100$ калит аниқланади. Бу калит эса, дастлаб шифрлаш жараёнида фойдаланилган k_3 га тенг.

Учинчи раунд калитини топиш учун зарур бўлган танлашларнинг максимал сони ($a = 2$, $b = 16$, $c = 16$) $n = 2*16*16 = 2^{10}$ ни ташкил қилади.

Хусусий ҳолда, уч раундли алгоритм учун интеграл криптотаҳлил алгоритми орқали сўнги раунд калитини топиш учун тузилган алгоритм орқали тўлиқ танлашлар сони алгоритмнинг ҳар бир такрор бажарилиши учун ($c=1$) $2 * 16 = 2^5$ тани ташкил этади. Юқоридаги мисолда эса алгоритм 8 марта ($c=2$) қайта бажарилди, яъни, учинчи раунд калитини топиш учун $2 * 16 * 2 = 2^6$ та танлаш ўтказиш талаб қилинди.

Мазкур алгоритм учун таклиф қилинган интеграл криптотаҳлил усули ёрдамида калитни топиш алгоритмидан уч раундли Кузнечик шифрлаш алгоритмида фойдаланилган калитни топиш учун ҳам фойдаланиш мумкин.

Кузнечик шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллашда, дастлаб алгоритмнинг ҳар бир акслантириши хусусиятларини кўриб чиқилди. Шунга кўра, Кузнечик акслантиришларининг турли хил кирувчи тўплам элементларини қандай ўзгартириши ўрганилди ҳамда кирувчи тўпламларнинг раундлардан чиқишдаги ўзгариши кузатилди. Кузатиш натижаларига кўра қуйидаги тасдиқ ва теоремалар ўринли.

Тасдиқ 1. Кузнечик шифрлаш алгоритмининг X акслантириши интеграл криптотаҳлил усулида танлаб олинган очиқ матнлар тўпламининг параметрларини ўзгартирмайди.

Тасдиқ 2. Кузнечик шифрлаш алгоритмининг S акслантириши интеграл криптотаҳлил усулида танлаб олинган очиқ матнлар тўпламининг параметрини фақат кирувчи тўплам элементи баланслашган бўлган ҳолатда баланслашмаганга акслантиради, қолган ҳолатларда тўплам параметрларига таъсир қилмайди.

Тасдиқ 3. Кузнечик алгоритми L акслантириши интеграл криптотаҳлил усулида танлаб олинган очиқ матнлар тўпламида битта актив байт бўлса барча элементлар актив байтларга, биттадан ортиқ актив байт бўлса ёки кирувчи тўпламда баланслашган элементлар мавжуд бўлса барча элементларни баланслашган тўпламга акслантиради.

Теорема 1. Кузнечик шифрлаш алгоритмида бир байти актив қолган байтлари пассив бўлган тўплам ёрдамида интеграл криптотаҳлил амалга оширилганда раунд киришидаги x тўплам ҳамда раунд чиқишидаги y тўпламлар учун қуйидаги тенгликлар фақат ва фақат учинчи раунд учун бир вақтда ўринли: $\sum_{i=0}^{255} x_i = 0$ ва $\sum_{i=0}^{255} y_i \neq 0$.

Тасдиқ 4. Кузнечик шифрлаш алгоритмида бир раундли дешифрлаш учун, яъни $x = S^{-1}(L^{-1}(X(y)))$ ни ҳисоблаш учун калит вариантларини тўлиқ танлашлар сони 2^{128} тани ташкил этади.

3 раундли алгоритм сўнгида чиқувчи массив y, учинчи раунд киришидаги массив эса x бўлса, $\sum x$ ни ҳисоблаш учун дастлаб қуйидаги кетма-кетлик бажарилиши зарур: $x = S^{-1}(L^{-1}(X(y)))$.

Юқоридаги Тасдиқ 3.4 га кўра ушбу амалларни бажариш калитларни мумкин бўлган барча вариантларини қўйиб топишдан самарали эмас, яъни, калит вариантларини тўлиқ танлашлар сони 2^{128} тани ташкил этади. S-KN1 шифрлаш алгоритми учун ишлаб чиқилган самарали алгоритм ёрдамида уч раундли Кузнечик алгоритмининг учинчи раундида фойдаланилган калитни

100 фоиз эҳтимоллик билан аниқлаш имконияти мавжуд.

Мазкур алгоритм ёрдамида уч раундли алгоритм учун интеграл криптотаҳлил усулида калитни топишнинг танлашлар сони алгоритмнинг ҳар бир такрор бажарилиши учун $16 * 256 = 2^{12}$ тани ташкил этади. Калитни топиш алгоритмида максимал танлашлар сони 2^{20} тани ташкил этади.

Диссертациянинг «**Кузнечик алгоритми акслантиришларининг ўрни алмашишининг интеграл криптотаҳлилга таъсири ва алгоритмни дастурий амалга ошириш»** номли тўртинчи боби Кузнечик шифрлаш алгоритмининг акслантиришлари кетма-кетлигининг таҳлил натижаларига таъсирини ўрганиш ва Кузнечик шифрлаш алгоритмини дастурий амалга ошириш усуллари таҳлилига бағишланган.

Кузнечик шифрлаш алгоритмининг *LXS*, *SLX*, *SXL* кетма-кетликдаги вариантлари учун интеграл криптотаҳлил натижалари ўрганилган ва улар стандартда келтирилган *LSX* кетма-кетлиги учун олинган натижалар билан таққосланган. *SLX* ва *SXL* кетма-кетликлари учун олинган натижалар шуни кўрсатадики, мазкур вариантлар учун бир байти актив бўлган очиқ матнлар тўпламини уч раундли шифрлаш натижасида иккинчи раунд киришида баланслашган ва чиқишида баланслашмаган бўлган тўпламни ҳосил қилиш мумкин. Бунинг сабаби, иккинчи раунддаги S акслантириши L акслантиришидан сўнг бажаралишидир. Ушбу моделларда фойдаланилган калитни топиш учун *LSX* кетма-кетлиги учун келтирилган алгоритмдан фойдаланиш самара бермайди. Шу сабабли алгоритмнинг мазкур вариантлар учун самарали бўлган кўриниши ишлаб чиқилди.

Уч раундли алгоритм акслантиришларининг стандартда келтирилган *LSX* варианти ҳамда *SLX* ва *SXL* вариантлари учун интеграл криптотаҳлил усули ёрдамида ва таклиф қилинган самарали алгоритмлардан фойдаланилганда талаб қилинадиган танлашлар сони қуйидаги 9 – жадвалда келтирилган.

9-жадвал

Уч раундли алгоритмда фойдаланилган калитларни аниқлаш учун талаб қилинадиган танлашлар сони

Аксланти-ришлар кетма-кетлиги	Бир раунд калитини аниқлаш учун талаб қилинадиган танлашлар сони	Самарали алгоритм ёрдамида бир раунд калитини аниқлаш учун талаб қилинадиган танлашлар сони	Самарали алгоритм ёрдамида уч раунд калитини аниқлаш учун талаб қилинадиган танлашлар сони
LSX	2^{128}	2^{20}	$3*2^{20}$
LXS	2^{128}	2^{20}	$3*2^{20}$
SLX	2^{128}	2^{20}	$3*2^{20}$
SXL	2^{128}	2^{20}	$3*2^{20}$

Алгоритмда акслантиришлар кетма-кетлигининг ўзгариши интеграл криптотаҳлил натижаларига таъсир қилмайди. Бундан келиб чиқадики қуйидаги тасдиқ ўринли:

Тасдиқ 5. Кузнечик шифрлаш алгоритмининг акслантиришлар кетма-кетлиги қандай бўлишидан қатъий назар алгоритмнинг интеграл криптотаҳлили натижаларига таъсир қилмайди.

Кузнечик алгоритмини дастурий томондан самарали амалга ошириш уни

татбиқ этишдаги, шунингдек, криптотаҳлил жараёнига ҳам таъсир қилиши мумкин бўлган муҳим жиҳатлардан ҳисобланади. Алгоритмни дастурий реализациясида L акслантиришни матрица кўринишида ифодалаш қулай ҳисобланади. L акслантиришнинг бундай ифодаланиши LFSR регистри орқали моделлаштиришга нисбатан анча тез ҳисобланишини таъминлайди. Дастур ишлаш вақтининг асосий қисмини L акслантириш эгаллайди. Шифрлаш ва матнни дастлабки ҳолатга ўгириш жараёнидаги операцияларни оптималлаштириш чекли майдонда векторни матрицага кўпайтириш амалини оптималлаштиришга боғлиқ. Бу амални тезлаштириш учун кўпинча олдиндан ҳисобланадиган LUT (Lookup Table) жадвалидан фойдаланилади.

L акслантириш LFSR (Linear feedback shift register) кўринишидаги регистр бўлгани боис, регистрининг *K* тактидан кейинги натижа*:*

$$\begin{pmatrix} a_{n-1}^* \\ a_{n-2}^* \\ a_{n-3}^* \\ \vdots \\ a_1^* \\ a_0^* \end{pmatrix} = \begin{pmatrix} c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_2 & c_1 & c_0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}^k \cdot \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} \quad \textbf{(9)}$$

LUT тузилиши. L акслантиришнинг ҳисобланиши **(9)** тенгламанинг хусусий ҳолатида $k=16$ га тенг бўлади.

$L_i(b): V_8 \to V_{128}$ акслантиришда ҳосил бўлган матрицанинг $i-$устуни: $L_i(b) = c_{i,15} \cdot b || c_{i,14} \cdot b || \dots || c_{i,0} \cdot b,\ b \in V_8$ бўлади.

У ҳолда L акслантиришни қуйидагича ифодалаш мумкин:

$$L(a) = L_{15}(a_{15}) \oplus L_{14}(a_{14}) \oplus \dots \oplus L_1(a_1) \oplus L_0(a_0)$$

LUT ўлчами 16×256 бўлиб, жадвалнинг ҳар бир элементи 16 байтдан иборат бўлган маълумотни ифодалайди. Бу ерда, $LUT[i][j]-$кириш векторининг $j-$ байтини L акслантириш матрицасидаги $i-$ устунига кўпайтириш натижаси. Шундай қилиб, LS акслантиришни ифодалаш учун блоклар билан LUT нинг 16 блоклари устида 2 модуль бўйича қўшиш амалини амалга ошириш зарур.

S ва L акслантиришларни бирлаштириш. Ҳар иккала акслантиришни бирлаштиришда қуйидаги ишлар амалга оширилади:

$L_i': V_8 \to V_{128}, i = 0, \dots, 15$ ҳисобланади:

$L_i'(b) = c_{i,15} \cdot \pi(b) || c_{i,14} \cdot \pi(b) || \dots || c_{i,0} \cdot \pi(b),\ b \in V_8.$

У ҳолда, L ва S акслантиришларни қуйидаги кўринишда ифодалаш мумкин: $LS(a) = L_{15}'(a_{15}) \oplus L_{14}'(a_{14}) \oplus \dots \oplus L_1'(a_1) \oplus L_0'(a_0)$.

LUT жадвалини ҳосил қилиш аввал кўриб ўтилганидек амалга оширилади. Фарқи шундаки, L ва S акслантиришлари битта акслантиришга бирлаштирилди. Энди барча учта акслантиришни битта LSX акслантириш сифатида реализация қилиш қийинчилик туғдирмайди.

Алгоритмни амалга оширишнинг таклиф қилинган бир қанча усуллари ўрганилди, қуйида ушбу усуллар учун оптималлаштириш натижаларини келтирилган (10-жадвал).

– **baseline** – L акслантиришнинг LFSR регистри ёрдамида реализацияси;
– **with LUT** – L акслантиришнинг (xmm регистридан фойдаланилмаган

ҳолда) LUT ёрдамида реализацияси;

– **LUT, xor** – LS акслантириш қиймати аввалдан ҳисобланган, LSX акслантиришларнинг битта функция сифатида реализацияси (xor учун вектор инструкциясидан фойдаланилган);

– **offset** – xmm регистри ва аралаштиришларнинг олдиндан ҳисобланган қийматидан фойдаланилган реализацияси;

– **AVX2 –** AVX2 регистри ёрдамида амалга оширилган реализация.

10-жадвал

ECB режимида шифрлаш тезлиги, Кб/с

CPU/ Усул	i3-4030u	i5-5200u	i5-7200u	i5-8250u
baseline	6144	9011	10444.8	11673.6
with LUT	54272	78848	101376	109568
LUT, xor	70656	101376	134144	142336
offset	80896	115712	138240	145408
AVX2	86016	123904	153600	162816

Олинган таҳлил натижаларидан ECB ва CFB режимлари учун AVX2 амалга ошириш усули ўринли бўлса, ECB ва CBC режимларида шифрлашда эса LUT, xor усули самарали деб топилган.

Юқорида кўриб ўтилган усуллардан ташқари оптималлаштиришнинг яна бир усули мавжудки, у криптографиянинг содда амаллари *and* ва *xor* амаллари асосига қурилган. Мазкур усулни параллел ҳисоблашларни амалга ошириш имконини берувчи дастурий тизимларда ёки қурилмаларда амалга оширилса самарали бўлади. Чунки, бу усулда ҳар битнинг қиймати бошқа битлардан мустақил равишда аниқланади.

ХУЛОСА

Диссертация иши криптотаҳлил усулларининг Кузнечик шифрлаш алгоритмига нисбатан қўлланилишини тадқиқига бағишланган бўлиб, унда олинган асосий натижалар қуйидагилардан иборат:

1. Кузнечик шифрлаш алгоритмидаги S алмаштириш жадвалининг умумий криптографик параметрлари шу турдаги бошқа алмаштириш жадвалларига нисбатан яхши танланганлиги, алгоритмнинг алгебраик криптотаҳлил усулига бардошлигини оширган.
2. Кузнечик алгоритмига нисбатан ўтказилган алгебраик криптотаҳлил усули 8 раундли ҳолат учун тузилган тенгламалар системасини сақлашда 2^{62} бит хотира ҳажмини талаб қилган.
3. Интеграл криптотаҳлил усули ва таклиф этилган алгоритм ёрдамида 3 раундли Кузнечик алгоритмининг калитини топиш учун талаб қилинадиган танлашлар сони 2^{20} тани ташкил қилган.
4. Актив байтларни қандай танланишидан қатъий назар ушбу тўплам L акслантиришидан икки марта ўтганидан кейинги S акслантиришдан ўтишида баланслашган тўпламни олиш имконияти мавжуд эмас.
5. Алгоритмни дастурий амалга ошириш усулларининг қиёсий таҳлилидан олинган натижалар ECB ва CFB режимлари учун AVX2 амалга ошириш усулини, ECB ва CBC режимларида шифрлашда эса LUT, xor усулини самарали эканлигини кўрсатди.

**НАУЧНЫЙ СОВЕТ DSc.03/30.12.2019.FM.01.02
ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ
НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА**

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

БОЙКУЗИЕВ ИЛХОМ МАРДАНОКУЛОВИЧ

ПРИМЕНЕНИЕ МЕТОДОВ КРИПТОАНАЛИЗА К АЛГОРИТМУ ШИФРОВАНИЯ КУЗНЕЧИК

05.01.05 – Методы и системы защиты информации. Информационная безопасность

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

ТАШКЕНТ - 2022

Тема диссертации доктора философии (PhD) по физика-математическим наукам зарегестрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2022.1.PhD/FM618.

Диссертация выполнена в Национальном университете Узбекистана имени Мирзо Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский(резюме)) размещен на веб-странице Научного совета (www.ik-fizmat.nuu.uz) и на Информационно-образовательном портале "ZiyoNet" (www.ziyonet.uz).

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физика-математических наук, профессор
Официальные оппоненты:	**Туйчиев Гулом Нумонович** доктор физика-математических наук
	Курьязов Давлатёр Матякубович доктор физика-математических наук
Ведущая организация:	**ГУП "UNICON.UZ" Центр научно-технических и маркетинговых исследований**

Защиты диссертации состоится "23" августа 2022 года в 16^{00} часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана. (Адрес: 100174, г.Ташкент, Алмазарский район, ул. Университетская, дом-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 № 98). (Адрес: 100174, г.Ташкент, Алмазарский район, ул. Университетская, дом-4. Тел:(+99871) 246-02-24).

Автореферат диссертации разослан "10" августа 2022 года.
(протокол рассылки № 7 от "13" июня 2022 года).

М.М. Арипов
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.

Г.У. Джураев
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.ф-м.н., доцент

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В глобальном масштабе особое значение придается проблемам криптоанализа алгоритмов симметричного блочного шифрования, в том числе вопросам криптоатак, направленных на определение ключа шифрования и выполнение криптоатак в зависимости от математических свойств отражений в алгоритме, шагов алгоритма, а также проводимых независимо от математических свойств и шагов. Изучение свойств преобразований, используемых в алгоритмах шифрования, вопросы оценки алгоритмов с использованием существующих методов криптоанализа считается исследовательским объектом научных исследований, проводимых в таких областях, как информационная безопасность, прикладная математика, криптография, криптоанализ и объектно-ориентированное программирование. Поэтому особое внимание уделяется непрерывному анализу стандартных алгоритмов в соответствии с требованиями устойчивости криптоанализа.

Сегодня информационная безопасность в мире обеспечивается программно-аппаратными средствами, а их криптомодули состоят из стандартных криптографических алгоритмов и протоколов, принятых на государственном или межгосударственном уровне. Среди этих криптографических алгоритмов алгоритмы симметричного шифрования обеспечивают конфиденциальность в процессе хранения, обработки и передачи информации. Поэтому анализ стандартных алгоритмов симметричного шифрования, их оценка современными методами криптоанализа является одним из целевых научных исследований.

В нашей стране в качестве научного и практического применения фундаментальных наук большое внимание уделяется таким важным направлениям, как информационная безопасность, создание надежных криптографических алгоритмов в области криптологии. Значительные результаты были достигнуты во многих научных исследованиях по использованию симметричных блочных алгоритмов шифрования при обеспечении конфиденциальности и целостности информации, созданию методов и алгоритмов, направленных на оценку симметричных блочных шифров методами криптоанализа. Проведение научных исследований на уровне международных стандартов по приоритетным направлениям «Алгебра и функциональный анализ, прикладная математика и математическое моделирование, вычислительная математика и дискретная математика, теория вероятностей и математическая статистика», были определены как основные задачи и направления деятелности. Для обеспечения исполнения постановления важное значение обретает, оценка стандартных алгоритмов шифрования методами криптоанализа и внедрение в практику полученных научных результатов.

Данное диссертационное исследование в определенной степени нацелено

на решение задач, обозначенных указами Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О Стратегии развития Нового Узбекистана на 2022-2026 годы» и от 7 февраля 2017 года УП-4947 «О стратегии действий дальнейшего развития Республики Узбекистан», постановлениями Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан», от 17 февраля 2017 года №ПП-2789 «О мерах по дальнейшему совершенствование организации, управления и финансирования научно-исследовательской деятельности Академии наук», от 20 апреля 2017 года №ПП-2909 «О мерах по дальнейшему развитию системы высшего образования», от 27 апреля 2018 года № ПП-3682 «О мерах по дальнейшему совершенствованию системы внедрения в практику инновационных идей, технологий и проектов», Постановление Кабинета Министров Республики Узбекистан от 21 ноября 2007 года №242 «Об утверждении положения о лицензировании деятельности по проектированию, разработке, реализации, ремонту и эксплуатации средств криптографической защиты информации», а также задач, определенных в других нормативно-правовых актах, связанных с данной деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствие с приоритетным направлением развития науки и технологий Республики IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Многие ученые проводили исследования по криптоанализу алгоритмов симметричного блочного шифрования и созданию надежных симметричных блочных шифров. В том числе Б.Шнайер, Ю.Додис, Н.Фергюсон, Дж.Келси, М.Мацуи, Л.Кнудсен, Н.Куртуа, Н.Харрис, Э.Бихам, А.Шамир, Дж.Л.Масси, Р.Олейников, Е.Ищукова, Л.Бабенко, О.Казимиров проводят исследования по созданию алгоритмов шифрования и криптографических преобразований также их оценке методам криптоанализа.

Оценка существующих алгоритмов симметричного блочного шифрования современными методами криптоанализа иследовались несколькими учеными. А. Жуков, Н. Молдовян, А. Молдовян оценили общие криптографические требования S-блоков алгоритма ГОСТ 28147-89. Этот алгоритм был оценен Л.Бабенко и Е.Ищуковой методом дифференциального криптоанализа, Б.Абдурахимовым и А.Саттаровым методами линейного дифференциального и алгебраического криптоанализа, Р.Алоевым и Б.Ахмедовым методами простого и расширенного слайд анализа. М.Арипов и Г.Туйчиев оценили алгоритмы симметричного блочного шифрования на основе сети Лея-Месси методами линейного, дифференциального криптоанализа. П. Хасанов, М. Каримов, Х. Хасанов разработали и

проанализировали блочный симметричный алгоритм шифрования на основе параметрической алгебры. Б.Абдурахимов и О.Алланов провели оценку стандартного алгоритма УзДСт1105:2009 методами алгебраического и интегрального криптоанализа.

Оценка современным методам криптоанализа алгоритма шифрования Кузнечика в стандарте ГОСТ Р 34.12-2015 рассмотрена в научных трудах следующих ученых, в том числе: дифференциальный анализ проведен Е.Толоманенко, в котором установлены дифференциальные свойства нелинейного преобразования S и линейного преобразования L; Линейный и дифференциальный криптоанализ для упрощенной версии алгоритма Кузнечика-S-KN2 выполнен Е.Ищуковой и др.; Г. Джураев и др. предложили параллельный алгоритм выполнения дифференциального криптоанализа для 3 раундов алгоритма Кузнечика; Алгебраический криптоанализ для алгоритма Кузнечика выполнил Э. Маро; алгоритм Кузнечик был оценен А.Бирюковым и др. методами мультимножественного алгебраического криптоанализа; Р.Аль-Тави и А.Юссеф оценили методами «Встреча в середине»; В.Кирюкин провел исследование по оценке атаками, зависящих от ключа. Оценку алгоритмов шифрования методом интегрального криптоанализа проводили следующие ученые, в том числе: Л. Кнудсен применил этот метод криптоанализа к алгоритму шифрования Square и получил соответствующие результаты; Дж. Деймен, Л. Кнудсен и В. Раймен оценили алгоритм шифрования AES как интегральный метод криптоанализа; Y.Hu, Y.Zhang и G.Xiao оценили алгоритм SAFER+ методом интегрального криптоанализа; Л. Кнудсен и Д. Вагнер провели научные исследования по применению метода интегрального криптоанализа.

Связанность диссертационного исследования с научно-исследовательскими планами высшего учебного заведения, в котором была выполнена диссертация. Диссертационное исследование выполнено согласно плану научно-исследовательских работ «Алгоритмы и программное обеспечение для решения задач прикладной математики» Национального университета Узбекистана.

Целью исследования является оценка устойчивости алгоритма симметричного шифрования Кузнечик с использованием интегральных и алгебраических методов криптоанализа.

Задачи исследования:

- анализ симметричных блочных алгоритмов шифрования и методов оценки их устойчивости;
- оценка алгоритма симметричного шифрования и алгоритма обучения методом алгебраического криптоанализа;
- оценка алгоритма симметричного шифрования и алгоритма обучения методом интегрального криптоанализа;
- разработка эффективного алгоритма применения метода интегрального криптоанализа к трехраундовому алгоритму симметричного

шифрования Кузнечика.

Объектом исследования является алгоритм симметричного шифрования и процессы криптоанализа.

Предметом исследования является оценка алгоритма симметричного шифрования Кузнечик и его учебного варианта с использованием методов интегрального и алгебраического криптоанализа.

Методы исследования. В процессе исследования использованы методы прикладной криптографии и криптоанализа, теория чисел, теория вероятностей, сравнительного анализа и методы объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

задача формирования линейных уравнений, представляющих преобразование L алгоритма симметричного шифрования Кузнечика, решена с использованием уравнений, представляющих умножение чисел в конечном поле;

криптостойкость алгоритма симметричного шифрования Кузнечик оценивалась путем формирования уравнений в направлении шифрования и дешифрования, что позволило уменьшить количество неизвестных методом алгебраического криптоанализа;

криптостойкость алгоритма симметричного шифрования Кузнечик оценивалась по набору открытых текстов с одним активным байтом методом интегрального криптоанализа;

разработан алгоритм определения раундовых ключей, используемых в процессе шифрования, методом интегрального криптоанализа для трехраундового симметричного алгоритма шифрования Кузнечика.

Практические результаты исследования заключаются в следующем:

разработано программное средство, позволяющее формировать уравнения преобразований алгоритма шифрования Кузнечик;

разработаны программные средства, позволяющие оценивать преобразований алгоритма шифрования Кузнечик с использованием методов алгебраического и интегрального криптоанализа;

разработано программное средство, позволяющее найти ключ, использованный в процессе шифрования трехраундового алгоритма шифрования Кузнечик, с помощью метода интегрального криптоанализа.

Достоверность результатов исследования. Достоверность результатов, полученных в диссертации, основана на строгости математических соображений, подтвержденных результатами численных исследований и реального и экспериментального анализа криптографических алгоритмов, полученных методами криптоанализа.

Научная и практическая значимость результатов исследования.

Научная значимость результатов исследования объясняется оценкой симметричных блочных шифров Кузнечик с использованием методов

интегрального и алгебраического криптоанализа.

Практическая значимость результатов исследования объясняется оценкой современных алгоритмов шифрования методами криптоанализа по результатам проведенных методов криптоанализа и по криптографическим характеристикам преобразований, основой в разработке новых алгоритмов шифрования и новых функций преобразования, а также возможностью применения методов криптоанализа в процессе обучения.

Внедрение результатов исследования. На основании полученных результатов по применению методов алгебраического и интегрального криптоанализа к алгоритму шифрования Кузнечик и оценки стойкости алгоритма:

научно-теоретические данные диссертационной работы, рекомендации по оценке устойчивости криптографических алгоритмов с использованием интегральных и алгебраических методов криптоанализа, решение задачи формирования линейных уравнений для преобразований алгоритма симметричного шифрования, подход, использованный при выполнении алгебраического криптоанализа, решения по применению методов алгебраического и интегрального криптоанализа к алгоритму шифрования «Кузнечик» были использованы при анализе методов криптоанализа в проекте «Создание криптографических алгоритмов», осуществляемом в ГУП «UNICON.UZ» (справка № 5 3/483. от 31 марта 2022 года ГУП «UNICON.UZ» - Центр научно-технических и маркетинговых исследований). Применение научных результатов дало возможность сформулировать уравнения, представляющие алгоритмы шифрования в процессе реализации методов линейного и алгебраического криптоанализа, уменьшить числа неизвестных в алгебраическом выражении алгоритма шифрования, оценить стойкости алгоритмов шифрования, используемых в национальных защищенных системах в ГУП «UNICON.UZ».

результаты оценки стойкости полученного в диссертации обучающего варианта алгоритма симметричного шифрования Кузнечика методами криптоанализа а также оценки стойкости алгоритма симметричного шифрования Кузнечика методами интегрального и алгебраического криптоанализа и подход к оценке стойкости обучающего варианта алгоритма симметричного шифрования Кузнечика методами криптоанализа были использованы при подобрание алгоритмов криптографической защиты информации и оценке криптостойкости в проекте №Ф706-17 - «Исследование применения биометро-криптографических технологий в информационных системах» (справка № 968/15-01 от 1 апреля 2022 года ТУИТ им. Мухаммада ал-Хоразмий). Применение научных результатов дало возможность подобрать алгоритмы криптографической защиты данных и оценить криптостойкости и изучить интегральные и алгебраические свойства преобразований алгоритмов симметричного блочного шифрования.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 3 международных и 3 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме диссертации опубликовано в общей сложности 15 научных работ, из них 9 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 6 – в иностранных и 3 – в республиканских журналах, а также получены 4 свидетельства о регистрации программных продуктов для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 119 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИСЕРТАЦИИ

В введении обоснованы актуальность и востребованность темы диссертации, показано соответствие с приоритетными направлениями развития науки и технологий Республики Узбекистан, формулируются цель и задачи, также объект и предмет исследования, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работах и структура диссертации.

В первой глава диссертации, озаглавленной как «**Алгоритмы шифрования стандарта ГОСТ Р 34.12.2015 и результаты их оценки методами криптоанализа**» описаны методы криптоанализа, используемые для оценки алгоритмов симметричного блочного шифрования, алгоритмы шифрования стандарта ГОСТ Р 34.12.2015 и результаты проведенного в отношении них криптоанализа.

Криптоаналитик стремится узнать больше о ключе шифрования в различных условиях, чтобы уменьшить область, в которой может быть ключ *K*. (вероятный, предположительный...). Л. Кнудсен классифицировал методы криптоанализа блочных шифров по объему и качеству получаемых данных следующим образом: *полный взлом; глобальная дедукция; частичная дедукция; информационная дедукция.*

В настоящее время при анализе симметричного блочного шифрования используется множество криптографических методов, среди которых можно отдельно привести следующие:

- метод дифференциального криптоанализа (differential cryptanalysis);
- метод линейного криптоанализа (linear cryptanalysis);
- метод линейно-дифференциального криптоанализа (linear-differential cryptanalysis);
- метод алгебраического криптоанализа (algebraic crypanalysis);
- метод интегрального криптоанализа (integral cryptanalysis).

В настоящем стандарте приведено описание двух базовых блочных шифров с длинами блоков $n = 128$ бит и $n = 64$ бит и длинами ключей $k = 256$ бит. Если описанный в настоящем стандарте шифр с длиной блока $n = 128$ бит назвать блочным шифром «Кузнечик» («Kuznyechik»), то шифр с длиной блока $n = 64$ бит можно назвать блочным шифром «Магма» («Magma»).

Результаты криптоанализа, выполненного по отношению алгоритмов Магма и Кузнечик, представлены в Таблице 1.

Таблица 1

Результаты криптоанализа современных симметричных шифров (D - количество выделенного открытого текста или зашифрованного текста, M - объем памяти или количество операций, T - затраченное время, R - количество расшифрованных раундов)

Алгоритмы шифрования / Методы криптоанализа	**Магма**	**Кузнечик**
Метод линейного криптоанализа	- R=32, $T=2^{173,8}$ и $D=2^{173,8}$. - полностью устойчивым стал после 5-го раунда.	- было установлено, что алгоритм полностью устойчив этому методу анализа.
Метод дифференциального криптоанализа	- полностью устойчивым стал после 6-го раунда. - для 32-го раунда с уязвимой таблицей S вероятность атаки была от 2^{-25} до 2^{-33}.	- R=3, $D= 2^{-108} + 6 * 2^{-120}$; - доказано устойчивость после 3-го раунда; - было установлено, что алгоритм полностью устойчив этому методу анализа.
Метод линейно-дифференциального криптоанализа	- устойчивым стал после 12-го раунда.	-
Метод алгебраического криптоанализа	- R=3, M=45,43 Гбайт; - устойчивым стал после 5-го раунда. - сложность атаки была равна 2^{44}.	- $T=2^{154.5}$, $M=2^{140}$; - сложность атаки для одного раунда была равна 2^{33}; - для трех раундового алгоритма SKN2 решать логические уровнения методом XL требовалось 236,33 секунды времени и 1,191 Гб оперативной памяти.
Интегральный криптоанализ по отношению к алгоритмам не проведен		
Другие методы атаки	- для “Сдвиговой атаке (slide attack)” предложен алгоритм параллельного программирования.	- метод атаки “Встречи посередине”: $D= 2^{113}$, $T=2^{140}$, $M=2^{153}$. - атака на основе “Связанных ключей”: $T=2^{32}$, $M=2^{30}$, $D=2^{16}$.

Во второй главе диссертации, озаглавленной как **«Оценка алгоритма шифрования Кузнечик с использованием метода алгебраического криптоанализа»**, осуществлены формирование уравнений относительно преобразований алгоритма шифрования Кузнечик, алгебраический

криптоанализ по отношению алгоритма обучения S-KN1 и алгоритма шифрования Кузнечик.

В преобразование L алгоритма шифрования Кузнечик входные байты умножаются на числа 148, 32, 133, 16, 194, 192, 251 и для этого сложно составить уравнения. Поэтому целесообразно, чтобы эти методы умножения выполнялись по частям. То есть можно выразить эти числа как сумму 2, 4, 8, 16, 32, 64, 128. Следовательно, эту задачу можно решить, представив умножение этих чисел в виде уравнения. Ниже приводится уравнение для умножения на 148 с использованием уравнений, полученных для этой цели:

$$\mathbf{148}(x_7, x_6, x_5, x_4, x_5, x_6, x_7, x_0) mod\ p(x) = |128 + 16 + 4|$$
$$= x_5, x_4, x_5 + x_3, x_6 + x_4 + x_2 + x_0, x_5 + x_3 + x_1, x_4 + x_2 + x_1$$
$$+ x_0, x_6 + x_3 + x_1, x_6 + x_2$$

Для остальных операций умножения на числа 133, 194, 192, 251 уравнения также формулируются в таком порядке:

148=128+16+4; 133=128+4+1; 194=128+64+2; 192=128+64; 251=128+64+32+16+8+2+1.

Уравнении, которые представляют вышеупомянутое преобразование L, можно использовать в методе алгебраического криптоанализа.

Для алгоритма S-KN1 при алгебраическом представлении полученных дробных элементов достаточно рассмотреть *X, S, L* – функции. Преобразование, влияющее на параметры уравнений, является отражением *S.*

***y=S(x)* - функция** – выполняет преобразование S, размером 4x4 бит (таблица замены является статичной).

По отношению этого преобразования можно построить алгебраические уровнения в прямом (шифровании) направлении, в обратном (перевод текста в исходное положение) направлении и комбинированные (с пониженным уровнем), а именно:

$$1.\quad y_i = F(x_1, x_2, \dots, x_4)\ ,\ i = 1,2, \dots ,8$$
$$2.\quad x_i = F(y_1, y_2, \dots, y_4)\ ,\ i = 1,2, \dots ,8 \qquad \mathbf{(1)}$$
$$3.\quad F(x_1, x_2, \dots, x_4, y_1, y_2, \dots, y_4) = 0$$

Анализ преобразования S алгоритма шифрования S-KN1 в целом приведен в следующей таблице:

Таблица 2

Криптографические показатели преобразования S алгоритма шифрования S-KN1

Аргументы	4	Регулярность	+	N(φ)	0	AI(f)	1
Балансированность	+	deg (f)	4	CI(f)	0	SAC(f)	-

Для преобразования S параметры уравнений, формированных методами, приведенными в (1), приведены в нижеследующей Таблице 3.

На следующем этапе метода алгебраического криптоанализа осуществляется формирование уравнений для раунда путем связывания уравнений, сгенерированных для каждого преобразования алгоритма.

Таблица 3

Параметры уравнений, составленные по отношению преобразования S алгоритма шифрования S-KN1

	DEG	NS	TS 4-ой степени	TS 3-ей степени	TS 2-ой степени	TS 1-ой степени
1-й метод	4	93	30	40	7	1
2-ой метод	4	93	30	48	-	-
3-й метод	2	36	-	-	20	1

Связи между преобразованиями относительно преобразования S, заданного в (1), в зависимости от методов построения системы уравнений можно построить следующими тремя способами.

1. $y = L(S(X(x)))$ **(2)**
2. $x = X\left(S^{-1}\left(L^{-1}(y)\right)\right)$ **(3)**
3. $F\left(L\left(S\left(X(x)\right)\right), y\right) = 0$ **(4)**

После этого осуществляется процесс взаимосвязи раундов, то есть на их основе формируется система общих уравнений, представляющая полный алгоритм шифрования.

Связывание раундов алгоритма Кузнечик можно осуществить по указанным выше признакам, используя следующие подходы:

1. Составлением уравнений, которые независимо выражают биты массива на выходе каждого раунда.

$$y_i = R_i(x_i) = L\left(S\left(X(x_i)\right)\right), y_{i+1} = R_{i+1}(x_{i+1}) = L\left(S\left(X(x_{i+1})\right)\right) = L\left(S\left(X(y_i)\right)\right) = L\left(S\left(X\left(L\left(S\left(X(x_i)\right)\right)\right)\right)\right) \textbf{(5)}$$

2. Составлением уравнений, которые независимо выражают биты на входе каждого раунда.

$$x_i = R^{-1}{}_i(y_i) = X\left(S^{-1}\left(L^{-1}\left((y_i)\right)\right)\right), x_{i-1} = R^{-1}{}_{i-1}(y_{i-1}) = X\left(S^{-1}\left(L^{-1}\left((y_{i-1})\right)\right)\right) = X\left(S^{-1}\left(L^{-1}\left((x_i)\right)\right)\right) = X\left(S^{-1}\left(L^{-1}\left(X\left(S^{-1}\left(L^{-1}\left((y_i)\right)\right)\right)\right)\right)\right) \textbf{(6)}$$

3. Использованием нового метода ввода переменных на входе каждого раунда.

$$F\left(L\left(A\left(X(x_{i+1})\right)\right), y_{i+1}\right) = F\left(S\left(A\left(X(y_i)\right)\right), y_{i+1}\right) = 0 \textbf{(7)}$$

Связывание раундов можно осуществить с помощью следующих методов:

1) с помощью уравнений, сформированных с использованием выражения **(2)**;

2) с помощью уравнений, сформированных с использованием выражения **(3)**;

3) уравнения, сформированные в первых двух раундах с использованием выражений **(2)** и **(5)** и в третьем раунде с использованием выражений **(3)** и **(6)**.

В нижеследующей Таблице 4 приведено количество неизвестных в системе уравнений, представляющей трехраундовый алгоритм, формированный с использованием приведенных выше уравнений:

Таблица 4

Параметры системы уравнений, представляющей трехраундовый алгоритм

Метод связывания раундов	**Количество неизвестных**
1-й метод	14232
2-й метод	9320
3-й метод	796

В алгебраическом представлении частичных элементов, созданных для алгоритма Кузнечик, S-функция является основным отражением, влияющим на параметры уравнений.

***y=S(x)* - функция** – выполняет преобразование S, размером 8x8 бит (таблица замены является статичной).

По отношению этого преобразования можно построить алгебраические уровнения в прямом (шифровании) направлении, в обратном (перевод текста в исходное положение) направлении и комбинированные (с пониженным уровнем), а именно:

1. $y_i = F(x_0, x_1, \dots, x_7)$, $i = 0,1, \dots, 7$
2. $x_i = F(y_0, y_1, \dots, y_7)$, $i = 0,1, \dots, 7$ **(8)**
3. $F(x_0, x_1, \dots, x_7, y_0, y_1, \dots, y_7) = 0$

Анализ преобразования S алгоритма шифрования Кузнечик в целом приведен в следующей Таблице 5:

Таблица 5

Криптографические показатели преобразования S алгоритма шифрования Кузнечик

Аргументы	8	Регулярность	+	N (f)	100	CI(f)	0	SAC(f)	-
Балансированность	+	deg (f)	7	N (φ)	100	AI(f)	3		

Для преобразования S параметры уравнений, формированных методами, приведенными в **(8)**, приведены в нижеследующей Таблице 6.

Таблица 6

Параметры уравнений, составленные по отношению преобразования S алгоритма шифрования Кузнечик

	DEG	NS	TS 7-ой степени	TS 6-ой степени	TS 5-ой степени	TS 3-ей степени
1- й метод	7	860	354	10	1	
2- й метод	7	860	360	5	-	
3- й метод	3	697	-	-	-	441

В алгоритме шифрования Кузнечик уравнения для одного раунда и связывающие раунды формируются методами такими же, как и в алгоритме S-KN1.

Когда связывание раундов выражается с помощью уравнений, сформированных с помощью Метода 3, который считается эффективным в

алгоритме обучения, параметры системы уравнений отображается в виде, приведенном в Таблице 7.

Объем памяти, необходимый для хранения системы, представляющей восьмираундовый алгоритм, равен 2^{62}.

Третья глава диссертации, озоглавленная как «**Оценка алгоритма шифрования Кузнечик с использованием метода интегрального криптоанализа**» посвещена реализации интегрального криптоанализа по отношению алгоритма обучения S-KN1, реализации эффективного алгоритма обнаружения ключа, использованного в алгоритме обучения S-KN1 и криптоанализа по отношению учеьного алгоритма Кузнечик.

Таблица 7

Параметры системы уравнений, представляющей алгоритм

Количество раундов	**Количество неизвестных**	**Требуемый объем памяти**	**Сложность решения** $\approx O^3$
2-й раунд	2^{17}	2^{25}	2^{51}
4-й раунд	2^{28}	2^{35}	2^{72}
6-й раунд	2^{41}	2^{48}	2^{123}
8-й раунд	2^{55}	2^{62}	2^{165}

Для того, чтобы применить интегральный метод криптоанализа к любому алгоритму шифрования, необходимо знать выбранные открытые тексты и соответствующий им специальный набор зашифрованных текстов. По определенным правилам отбора набора открытых текстов, для применение интегрированного метода криптоанализа к алгоритму шифрования S-KN1 выбирался набор простых текстов и выполнялось отслеживание.

В процессе наблюдения было установлено, что преобразование S в первом раунде алгоритма не распределяет активные фрагменты, а также не влияет на баланс delta набора. L преобразование, однако, распределяет одну активную часть в столбце на две активные части. X преобразование также не влияет на баланс, как и не распределяет активную часть. Где можно увидеть, что только L преобразования влияют на количество активных частей в наборе.

Аналогично для последующего раундов алгоритма шифрования S-KN1 наблюдается изменение набора.

Даже после второго раунда набор остается сбалансированным. Изменение наблюдаемого алгоритма шифрования набора после 3-го раунда приведено в нижеследующей Таблице 8.

Во входе 3-го раунда рассматриваемого алгоритма шифрования имеется сбалансированный элемент наблюдаемого набора, который позволяет идентифицировать ключ раунда, используемый в 4-м раунде алгоритма шифрования. На этом шаге можно остановить первый этап криптоанализа. Следующим шагом в криптоанализе является определение вариантов ключа, в этом процессе также известен набор зашифрованного текста в конце 3-го раунда, который считается необходимым.

Таблица 8

Изменения наблюдаемого набора после 3-го раунда

Отоб-ие	Значение в концк 2-го раунда	3-й раунд		
		S	L	X
1-й блок	0011 0000	0111 0011	1010 1010	0011 0110
2-й блок	0110 1110	0101 1101	0011 0010	1010 1110
3-й блок	0011 0100	0111 1111	1101 0110	0100 1010
4-й блок	0000 0100	0011 1111	1110 1010	0111 0110
5-й блок	0010 1111	1010 1000	0101 0101	1100 1001
6-й блок	0001 0111	0110 1011	0101 0001	1100 1101
7-й блок	1110 1100	1101 0100	1101 0000	0100 1100
8-й блок	1000 0100	0010 1111	1010 1001	0011 0101
9-й блок	0100 0101	1111 0000	1001 0010	0000 1110
10-й блок	1001 1100	1100 0100	1001 0011	0000 1111
11-й блок	1000 1111	0010 1000	0011 1110	1010 0010
12-й блок	1011 0111	1110 1011	0011 1010	1010 0110
13-й блок	1011 1010	1110 0001	1110 0000	0111 1100
14-й блок	0000 1010	0011 0001	1111 0100	0110 1000
15-й блок	1001 1001	1100 1100	0010 1011	1011 0111
16-й блок	1111 0110	1000 0101	1001 1110	0000 0010
(XOR)∑=	0000 0000	0011 1000	0111 1101	0111 1101

Следующий процесс криптоанализа, то есть определение значения ключа, используемого в последнем раунде алгоритма шифрования, осуществляется путем ведения статистики, зная наличие активных (или пассивных) байтов в наборе, включенном в последний раунд, и поступающую информацию из последнего раунда (зашифрованный текст).

По методу интегрального криптоанализа, по сути, в 3-х раундовом алгоритме S-KN1 для определения значение ключа последнего раунда необходимо расшифровать полный набор зашифрованных текстов на один раунд с методом полного выбора подбора возможных вариантов ключа последнего раунда.

Как видно из этой последовательности шагов, процесс преобразования набора шифров не так эффективен, как полный подбор ключевых вариантов. Однако, используя свойства алгоритма преобразования, можно добиться эффективного результата.

Для алгоритма предложен эффективный алгоритм применения метода интегрального криптоанализа и нахождения ключа.

Алгоритм поиска ключа в интегральном методе криптоанализа для трехраундового алгоритма S-KN1 выглядит следующим образом:

1. Выберается набор открытых текстов, один байт которого активный, остальные байты пассивные;

2. Осуществляется 3-х раундовое шифрование для всех массивов набора;

3. Рассчитываются значения $a = L^{-1}(y)$ для всех массивов полученного набора зашифрованных текстов;

4. Осуществляется проверка всех (от 0000 0000 до 1111 1111) возможных

для принятия вариантов k' ($k' = L^{-1}(k)$) и равенства $\sum x_i = 0$ для всех элементов $x_i = S^{-1}(a_i \oplus k'_i)$ ($i = 0,1$) набора x;

5. Выберается варианты, удовлетворяющие уравнению и принимается в качестве соответствующего байта k';

6. Повторять шаги 1-5 до тех пор, пока каждый байт k' не примет единственное значение, и каждый раз брать пересечение ранее сформированных вариантов с принятыми вариантами для одного байта k'.

7. Рассчитать $L(k')$ и объявить как ключ, использованного в конце трентьего раунда.

Количество выборов, сделанных для поиска ключа к третьему раунду этого алгоритма, определяется с помощью выражения: $n = a * b * c$

Где, a - количество элементов набора зашифрованного текста, b - количество зашифрованных текстов, c - количество выбранных наборов, состоящих из активных и пассивных частей.

На основе предложенного алгоритма было создано специальное программное обеспечение, осуществлен процесс нахождения ключа, использованного в рассмотренном выше примере.

В результатах, полученных с помощью программного обеспечения, вариантов, принятых в качестве кандидатов на первый полубайт $k^{'}$, было четыре (**0011, 1001, 1101 и 1111**), а кандидатов на второй полубайт — два (**0011 и 1110**). Поэтому, последовательности, выполненные выше, повторялись для другого набора открытых текстов, как указано на шаге 6, до тех пор, пока ключи-кандидаты не образовали один.

Результаты показали, что вариантов, принятых в качестве кандидатов на первую половину байта $k^{'}$, было два (**0100 и 1101**), а кандидатов на вторую половину байта — восемь (**0000, 0010, 0101, 0111, 1001, 1011, 1100 и 1110**). При получении пересечения вариантов значения $k^{'}$ формируются **1101** для первого полубайта и **1110** для второго полубайта. Итак, определяется ключ $k^{'} = 11011110$ и $k = L(k^{'}) = 10011100$. Этот ключ равен k_3, который изначально использовался в процессе шифрования.

Максимальное количество вариантов, необходимое для поиска ключа третьего раунда, равно ($a = 2$, $b = 16$, $c = 16$) $n = 2 * 16 * 16 = 2^{10}$. В частности, для трехроундового алгоритма через алгоритм, настроенный для поиска ключа последнего раунда с использованием встроенного алгоритма криптоанализа точное количество выборов для каждой повторной реализации составляет ($c = 1$) $2 * 16 = 2^5$. В приведенном выше примере алгоритм был выполнен 8 раз (), то есть для нахождения ключа третьего раунда требуется провести выборку $2 * 16 * 2 = 2^6$ раз.

С помощью метода интегрального криптоанализа, предложенного для этого алгоритма, алгоритм нахождения ключа можно также использовать для нахождения ключа, используемого в трехраундовом алгоритме шифрования

Кузнечик.

При применении метода интегрального криптоанализа к алгоритму шифрования Кузнечик в первую очередь рассматривались характеристики каждого преобразования алгоритма. Соответственно, изучалось, как преобразования Кузнечика изменяют элементы различных входящих наборов, и наблюдались изменения выхода входящих наборов из раундов. По результатам наблюдения уместным считается следующее теоремы и подтверждения.

Подтверждение 1. Преобразование X алгоритма шифрования Кузнечика не изменяет параметры набора открытого текста, выделенного методом интегрального криптоанализа.

Подтверждение 2. Преобразование S алгоритма шифрования Кузнечика преобразует параметр набора открытого текста, выбранный методом интегрального криптоанализа в несбалансированный только в том случае, если входящий элемент набора является сбалансированным, в остальных случаях он не влияет на параметры набора.

Подтверждение 3. Преобразование L алгоритма шифрования Кузнечика преобразует все элементы в активные байты, если в наборе открытого текста есть один активный байт, и все элементы в сбалансированный набор, если активных байтов больше одного или есть сбалансированные элементы во входящем наборе.

Теорема 1. В алгоритме шифрования Кузнечика при выполнении интегрального криптоанализа с использованием множества, в котором один байт активен, а остальные байты пассивный, для множеству *x* на входе раунда и для множеству *y* на выходе, следующие уравнения действительны только и только для третьего раунда одновременно: $\sum_{i=0}^{255} x_i = 0$ ва $\sum_{i=0}^{255} y_i \neq 0$.

Подтверждение 4. Количество полных выборов вариантов ключа для однораундовой дешифровки в алгоритме шифрования Кузнечика, т.е. для вычисления $x = S^{-1}(L^{-1}(X(y)))$, равно 2^{128} .

Если выходной массив в конце 3-раундового алгоритма равен y, а массив на входе третьего раунда равен x, то для вычисления $\sum x$ необходимо сначала выполнить следующую последовательность: $x = S^{-1}(L^{-1}(X(y)))$.

Согласно приведенному выше Подтверждению 3.4, выполнение этих шагов не более эффективно, чем освобождение всех возможных вариантов ключей, т. е. количество полных выборов вариантов ключей равно 2^{128}. Используя эффективный алгоритм, разработанный для алгоритма шифрования S-KN1, можно со 100-процентной вероятностью идентифицировать ключ, используемый в третьем раунде трехраундового алгоритма Кузнечика.

Количество вариантов поиска ключа в методе интегрального криптоанализа для трехроундного алгоритма с использованием этого алгоритма составляет $16 * 256 = 2^{12}$ для каждого повторения алгоритма. Максимальное количество выборок в алгоритме поиска ключей составляет 2^{20}.

Четвертая глава диссертации, озоглавленная как «**Влияние изменения последовательности преобразовании алгоритма Кузнечика на интегральный криптоанализ и программное реализация алгоритма»** посвящена исследованию влияния последовательности преобразований алгоритма шифрования Кузнечик на результаты анализа и анализу методов программной реализации алгоритма шифрования Кузнечик.

Были изучены результаты интегрального криптоанализа для вариантов последовательностей *LXS, SLX, SXL* алгоритмов шифрования Кузнечик, и они были сравнены с результатами, полученными для стандартных последовательностей *LSX*. Результаты для последовательностей *SLX* и *SXL* показывают, что набор открытых текстов, активных на один байт для этих вариантов сбалансирован во входе второго раунда в результате трех раундового шифрования, и на выходе может сгенерировать несбалансированный набор. Это связано с тем, что преобразование S во втором раунде выполняется после преобразования L. Использование алгоритма, приведенного для последовательности *LSX* является неэффективным для того, чтобы найти ключ, используемый в этих моделях. По этой причине для этих вариантов разработан эффективный вид алгоритма.

Вариант LSX, приведенный в стандарте трехраундового алгоритма преобразования, а также количество виборок, необходимых при использовании предложенных эффективных алгоритмов с использованием метода интегрального криптоанализа для вариант *LSX*, приведеного в стандарте трехраундового алгоритма преобразования и вариантов *SLX* и *SXL* приведены в нижеследующей Таблице 9.

Таблица 9

Количество выборок, необходимых для определения ключей, используемых в трехраундовом алгоритме

Последовательность преобразований	Количество виборок, требуемых для определения ключа одного раунда	Количество виборок, требуемых для определения ключа одного раунда с использованием эффективного алгоритма	Количество виборок, требуемых для определения ключа третьего раунда с использованием эффективного алгоритма
LSX	2^{128}	2^{20}	$3*2^{20}$
LXS	2^{128}	2^{20}	$3*2^{20}$
SLX	2^{128}	2^{20}	$3*2^{20}$
SXL	2^{128}	2^{20}	$3*2^{20}$

Изменения последовательности преобразований в алгоритме не влияют на результаты интегрального криптоанализа. Отсюда следует, что следующее утверждение является подходящим:

Подтверждение 5. Алгоритм шифрования Кузнечика не влияет на результаты интегрального криптоанализа алгоритма независимо от последовательности преобразований.

Эффективная программная реализация алгоритма Кузнечик является

важным аспектом во внедрении, а также в возможности влияния в процесс криптоанализа. В программной реализации алгоритма удобно представить преобразование L в виде матрицы. Такое выражение отражения L гарантирует, что оно вычисляется намного быстрее, чем моделирование через регистр LFSR.

Преобразование L занимает основную часть времени работы программы. Оптимизация операций в процессе шифрования и перевода текста в исходное положение зависит от оптимизации операции умножения вектора на матрицу в конечной области. Чтобы ускорить эту операцию, часто используется предварительно рассчитанная таблица LUT (Lookup Table).

Поскольку преобразование L является регистром в форме LFSR (Linear feedback shift register), результат регистра после такта *K* равен*:*

$$\begin{pmatrix} a_{n-1}^* \\ a_{n-2}^* \\ a_{n-3}^* \\ \vdots \\ a_1^* \\ a_0^* \end{pmatrix} = \begin{pmatrix} c_{n-1} & c_{n-2} & c_{n-3} & \dots & c_2 & c_1 & c_0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}^k \cdot \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} \textbf{(9)}$$

Структура LUT. Расчет преобразования L равен *k=16* в частном случае уравнения **(9)**.

$L_i(b): V_8 \to V_{128}$ - i −столбец матрицы, полученный в преобразовании: $L_i(b) = c_{i,15} \cdot b || c_{i,14} \cdot b || \dots || c_{i,0} \cdot b$, $b \in V_8$.

В этом случае преобразование L можно выразить следующим образом:

$$L(a) = L_{15}(a_{15}) \oplus L_{14}(a_{14}) \oplus \dots \oplus L_1(a_1) \oplus L_0(a_0)$$

Размер LUT составляет 16×256, и каждый элемент таблицы представляет 16 байтов данных. Где, $LUT[i][j]$ − результат умножения j −байта входного вектора на i −столбец матрицы преобразования L. Таким образом, необходимо выполнить операцию сложения над 2 модулями на 16 блоках LUT с блоками для выражения отражения LS.

Объединение оображений S и L. При объединении обоих преобразований производится следующие действия:

Расчитывается $L'_i: V_8 \to V_{128}, i = 0, \dots, 15$:

$L'_i(b) = c_{i,15} \cdot \pi(b) || c_{i,14} \cdot \pi(b) || \dots || c_{i,0} \cdot \pi(b)$, $b \in V_8$.

В этом случае преобразования L и C можно выразить следующим образом: $LS(a) = L'_{15}(a_{15}) \oplus L'_{14}(a_{14}) \oplus \dots \oplus L'_1(a_1) \oplus L'_0(a_0)$.

Формирование таблицы LUT выполняется, как описано ранее. Отличие в том, что преобразования L и C объединяются в одно преобразование. Теперь реализовать все три преобразования как одно преобразование LSX не составить труда.

Был изучен ряд предложенных методов реализации алгоритма, и ниже представлены результаты оптимизации этих методов (Таблица 10).

– **baseline** – реализация преобразования L с помощью регистра LFSR;

– **with LUT** – реализация преобразования L с помощью LUT

(использованием регистра xmm);

– **LUT, xor** – реализация как одна функция преобразования LSX (для xor использован инструкция вектора), преобразование LS расчитан заранее;

– **offset** – реализация с использованием регистра xmm и заранее расчитанным значением преобразования;

– **AVX2 –** реализация с помощью регистра AVX2.

Таблица 10

Скорость шифрования в режиме ECB, Мб/с

CPU/ Метод	i3-4030u	i5-5200u	i5-7200u	i5-8250u
Baseline	6144	9011	10444.8	11673.6
with LUT	54272	78848	101376	109568
LUT, xor	70656	101376	134144	142336
Offset	80896	115712	138240	145408
AVX2	86016	123904	153600	162816

Результаты анализа показали, что метод реализации AVX2 подходит для режимов ECB и CFB, а метод LUT эффективен для шифрования в режимах ECB и CBC

В дополнение к методам, рассмотренным выше, существует еще один метод оптимизации, который основан на простых операциях криптографии *and* и *xor*. Этот метод наиболее эффективен при выполнении на программных системах или устройствах, допускающих параллельные вычисления. Потому что в этом методе значение каждого бита определяется независимо от других битов.

ЗАКЛЮЧЕНИЕ

Диссертация посвящена исследованию применения методов криптоанализа к алгоритму шифрования Кузнечик, основные результаты которого заключаются в следующем:

1. Общие криптографические параметры таблицы замены S в алгоритме шифрования Кузнечик хорошо подобраны по сравнению с другими таблицами замены этого типа, повышена устойчивость алгоритма к алгебраическим методам криптоанализа.
2. Метод алгебраического криптоанализа, выполненный по отношению алгоритма Кузнечик, требовал 2^{62} бита памяти для хранения системы уравнений, построенной для 8-раундового состояния.
3. Количество выборок, необходимых для нахождения ключа к 3-раундовому алгоритму Кузнечика с использованием метода интегрального криптоанализа и предложенного алгоритма, составило 2^{20}.
4. Независимо от того, как выбраны активные байты, невозможно получить сбалансированный набор после преобразования S после того, как этот набор дважды проходит преобразование L.
5. Результаты сравнительного анализа методов программной

реализации алгоритма показали, что метод реализации AVX2 эффективен для режимов ECB и CFB, а метод LUT, xor эффективен для шифрования в режимах ECB и CBC.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.03/30.12.2019.FM.01.02 NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN

BOYKUZIEV ILKHOM MARDANOKULOVICH

APPLICATION OF CRYPTANALYSIS METHODS TO KUZNYECHIK ENCRYPTION ALGORITHM

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-2022

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Comission at the Cabinet of Ministers of the Republic og Uzbekistan under number B2022.1.PhD/FM618.

Dissertation has been prepared at National University of Uzbekistan.

The abstract of the dissertation is posted in three languages (uzbek, russion, 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 Matematical Sciences, Professor
Official opponents:	**Tuychiev Gulom Numonovich** Doctor of Physical and Matematical Sciences
	Kuryazov Davlatyor Matyakubovich Doctor of Physical and Matematical Sciences
Leading organization:	**SUE «UNICON.UZ» Scientific-engineering and Marketing researches center**

Defense will takr place "23" August 2022 at 16^{00} ft the meeting of Scientific Council number DSc.03/30.12.2019.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 in possible to review in Information-resource centre at National University of Uzbekistan (is registred № 98). (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 246-02-24).

Abstract of dissertation sent out on "10" August 2022 year
(Mailing report № 7 on "13" June 2022 year)

M.M. Aripov
Chairman of Scientific council on award of scientific degress, D.F-M.S., professor

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

G.U. Jurayev
Chairman of Scientific seminar under scientific council on award of scientific degress, D.F-M.S., docent

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to assess the stability of the Kuznyechik symmetric encryption algorithm using the methods of integral and algebraic cryptanalysis.

The object of the research work is Kuznyechik symmetric encryption algorithms and cryptanalysis processes.

The scientific novelty of the research work is as follows:

the problem of forming linear equations representing the transformation L of Kuznyechik symmetric encryption algorithm is solved using equations representing the multiplication of numbers in a finite field;

the cryptographic strength of the Kuznyechik symmetric encryption algorithm was estimated by forming equations in the direction of encryption and decryption, which made it possible to reduce the number of unknowns by the method of algebraic cryptanalysis;

the cryptographic strength of the Kuznyechik symmetric encryption algorithm was evaluated by a set of plaintexts with one active byte by the method of integral cryptanalysis;

An algorithm for determining the round keys used in the encryption process was developed using the integral cryptanalysis method for the Kuznyechik three-round symmetric encryption algorithm.

Implementation of the research results. Scientific results on the evaluation of the Kuznyechik algorithm by the methods of algebraic and integral cryptanalysis are put into practice in the following areas:

scientific and theoretical data of the dissertation work, recommendations for assessing the stability of cryptographic algorithms using integral and algebraic methods of cryptanalysis, solving the problem of forming linear equations for transformations of the symmetric encryption algorithm, the approach used in performing algebraic cryptanalysis, solutions for applying the methods of algebraic and integral cryptanalysis to the algorithm " Kuznyechik" ciphers were used in the analysis of cryptanalysis methods in the project "Creation of cryptographic algorithms", carried out at SUE "UNICON.UZ" (reference No. 5 3/483. dated March 31, 2022 SUE "UNICON.UZ" - Center for Scientific and Technical and marketing research). The application of scientific results made it possible to formulate equations representing encryption algorithms in the process of implementing methods of linear and algebraic cryptanalysis, to reduce the number of unknowns in the algebraic expression of the encryption algorithm, to evaluate the strength of encryption algorithms used in national secure systems in SUE "UNICON.UZ".

the results of assessing the security of the training version of Kuznyechik symmetric encryption algorithm obtained in the dissertation by cryptanalysis methods, as well as assessing the security of the Kuznyechik symmetric encryption algorithm by methods of integral and algebraic cryptanalysis and the approach to assessing the security of the training version of the Kuznyechik symmetric encryption algorithm by cryptanalysis methods were used in the selection of algorithms for cryptographic information protection and evaluation cryptographic

strength in project No. Ф706-17 - “Research on the use of biometric-cryptographic technologies in information systems” (reference No. 968/15-01 dated April 1, 2022, TUIT named after Muhammad al-Khwarizmi). The application of scientific results made it possible to select cryptographic data protection algorithms and evaluate cryptographic strengths and study the integral and algebraic properties of transformations of symmetric block cipher algorithms.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendix. The volume of the thesis is 119 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (Часть I; Part I)

1. Бойқузиев И.М. Кузнечик шифрлаш стандартининг S ва L акслантиришлари учун чизиқли тенгламалар тузиш муаммоси ва ечими // Муҳаммад ал-Хоразмий авлодлари илмий-амалий ва ахборот-таҳлилий журнал, 2021, № 2(16), 58-62 бет. (05.00.00 №10)

2. Бойқузиев И.М. Кузнечик шифрлаш алгоритми реализациясининг оптимал усуллари // Наманган давлат университети илмий ахборотномаси, 2021, № 11, 24-30 бет. (01.00.00 №14)

3. B. Abdurakhimov, I. Boykuziev, Z. Khudoykulov and O. Allanov "Application of the algebraic cryptanalysis method to the Kuznyechik encryption algorithm" // International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 01-06, doi: 10.1109/ICISCT52966.2021.9670359. (№3, Scopus. ОАК Раёсатининг 30.10.2021 йилдаги №308/6–сон қарори)

4. B. Abdurakhimov, I. Boykuziev, O. Allanov and B. Xidirov "Differential characteristics of reflections of Kuznyechik encryption algorithm" // 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670212. (№3, Scopus. ОАК Раёсатининг 30.10.2021 йилдаги №308/6–сон қарори)

5. Адбурахимов Б.Ф., Бойқузиев И.М., Худойқулов З.Т., Алланов О. Кузнечик симметрик шифрлаш алгоритми ўқув варианти учун интеграл криптотаҳлил усулининг қўлланилиши // Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, «UNICON.UZ» ДУК - Фан-техника ва маркетинг тадқиқотлари маркази. Ахборотқоммуникациялар: Тармоқлар-технологиялар-ечимлар журнали, 2022, № АК: ТТЕ №1 (61)/2022, 35-42 бет. (05.00.00 №2)

II бўлим (Часть II; Part II)

1. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. Analysis of algebraic properties of transformation of O’z DSt 1105:2009 algorithm // International Conference on Information Science and Communications Technologies (ICISCT), 2019, pp. 1-3.

2. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. Algebraic Cryptanalysis of O’z DSt 1105:2009 Encryption Algorithm // International conference on Information Sience and Communication Technologies (ICISCT), 2020, pp. 1-6, doi: 10.1109/ICISCT50599.2020.9351469.

3. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. Differential Collisions in SHA-1 // International conference on Information Sience and Communication Technologies (ICISCT), 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351441.

4. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M. A Novel Secure RNG Based On Three Entropy Sources // International Journal of Advanced Science and Technology, 2020, Volume 29, No. 5, pp. 12397-12412. (05.00.00 №17 IF=0.41)

5. Бойқузиев И.М. ГОСТ Р 34.12-2015 шифрлаш стандарти учун криптотаҳлил усулларининг қўлланилиши // Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти, Республика илмий-техник анжумани, 4-5 март, 2021, ТАТУ, Тошкент, 2-қисм, 251-254 бет.

6. Boykuziev I. M. Application of the method of algebraic cryptanalysis to the encryption algorithm S-KN1 // The 6th International scientific and practical conference ―Topical issues of modern science, society and education, December 26-28, 2021, SPC “Sci-conf.com.ua”, Kharkiv, Ukraine, pp. 505-511.

7. Boykuziev I. M. Formation of linear equations for L-reflection of the Kuznyechik algorithm // The 5th International scientific and practical conference “Innovations and prospects of world science”, December 29-31, 2021, Perfect Publishing, Vancouver, Canada. pp. 364-368.

8. Bakhtiyor Abdurakhimov, Ilkhom Boykuziyev, Javokhir Abdurazzokov Encryption systems and the history of their development // Scientific collection «INTERCONF» | № 95. Scientific goals and purposes in XXI century, January 19-20, 2022, ISSN 2709-4685, Seattle, USA, doi: 10.51582/interconf.19-20.01.2022.085

9. З. Худойқулов, И. Бойқўзиев Кузнечик шифрлаш алгоритмини криптотаҳлил усулларига баҳолаш натижалари // Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти. Республика илмий-техник анжумани, 10-11 март, 2022, ТАТУ, Тошкент, 1-қисм, 344-346 бет.

10. И. Бойқўзиев, Б. Хидиров Интеграл криптотаҳлил усулининг кузнечик шифрлаш алгоритмининг ўқув вариантига қўлланилиши // Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти. Республика илмий-техник анжумани, 10-11 март, 2022, ТАТУ, Тошкент, 1-қисм, 347-349 бет.

11. Бойқўзиев И.М., Абдурахимов Б.Ф., Худойқулов З. Т., Алланов О. Уч раундли Кузнечик шифрлаш алгоритмининг шифрлаш калитини топиш дастури // Дастурга гувоҳнома № DGU 13596, 16.12.2021.

12. Бойқўзиев И.М., Абдурахимов Б.Ф., Каримов А.А., Турсунов О.О. Кузнечик шифрлаш алгоритми дастурий таъминоти// Дастурга гувоҳнома № DGU 13577, 16.12.2021.

13. Бойқўзиев И.М., Худойқулов З. Т., Узакова М.А., Мўминова С.Ш. Кузнечик шифрлаш алгоритми L акслантиришига тенгламалар шакллантириш дастури // Дастурга гувоҳнома № DGU 13595, 16.12.2021.

14. Бойқўзиев И.М., Алланов О., Холимтаева И.У., Мўминова С.Ш. Кузнечик шифрлаш алгоритмига интеграл криптотаҳлил ўтказиш дастури // Дастурга гувоҳнома № DGU 13597, 16.12.2021.

Автореферат Ўзбекистон Миллий университетининг «ЎзМУ хабарлари»
илмий журнали таҳририятида таҳрирдан ўтказилди.

Босмахона лицензияси:

9338

Бичими: 84x60 $^{1}/_{16}$. «Times New Roman» гарнитураси.
Рақамли босма усулда босилди.
Шартли босма табоғи: 3,75. Адади 100 дона. Буюртма № 1/22.

Гувоҳнома № 851684.
«Tipograff» МЧЖ босмахонасида чоп этилган.
Босмахона манзили: 100011, Тошкент ш., Беруний кўчаси, 83-уй.