А
А 51

ЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ
ЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ
/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ
Г АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

АЛЛАНОВ ОРИФ МЕНГЛИМУРАТОВИЧ

СИММЕТРИК ШИФРЛАШ АЛГОРИТМИНИ ТАКОМИЛЛАШТИРИШ ВА КРИПТОТАҲЛИЛ УСУЛЛАРИ ЁРДАМИДА БАҲОЛАШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2021

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

АЛЛАНОВ ОРИФ МЕНГЛИМУРАТОВИЧ

СИММЕТРИК ШИФРЛАШ АЛГОРИТМИНИ ТАКОМИЛЛАШТИРИШ ВА КРИПТОТАҲЛИЛ УСУЛЛАРИ ЁРДАМИДА БАҲОЛАШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2021

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2021.2.PhD/T1940 рақам билан рўйхатга олинган.

Диссертация Тошкент ахборот технологиялари 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:	**Жўраев Ғайрат Умарович** физика-математика фанлари доктори, доцент
	Юсупов Боходир Караматович техника фанлари бўйича фалсафа доктори (PhD)
Етакчи ташкилот:	**«UNICON.UZ»-фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 Илмий кенгашнинг 2021 йил «22» июня соат 0900 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (205 рақам билан рўйхатга олинган). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2021 йил «___» _____ да тарқатилди.
(2021 йил «___» _____ даги ___ рақамли реестр Обаённомаси.)

Р.Х. Хамдамов
Илмий даражалар берувчи илмий кенгаш раиси, техника фанлари доктори, профессор

Ф.М. Нуралиев
Илмий даражалар берувчи илмий кенгаш илмий котиби, техника фанлари доктори, доцент

С.К. Ганиев
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, техника фанлари доктори, профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳон миқёсида ахборотни ҳимоялаш масалаларини ечишда криптографик ҳимоя ўзининг юқори ишончлилиги ва кафолатлиги билан етакчи ўринни эгалламоқда. Хусусан, Accenture компанияси тақдим этган маълумотга кўра «2019-йилда ташкилотлар томонидан криптографик ҳимоя механизмларидан фойдаланиш натижасида 0,85 миллион АҚШ доллар тежалган»[1]. Ахборотнинг конфиденциаллик, яхлитлик хусусиятларини таъминлашда ва рад этишдан ҳимоялашда криптографик ҳимоя муҳим аҳамият касб этгани боис, криптографик алгоритмларнинг бардошлигини баҳолаш ҳозирги кундаги долзарб масалалардан бири ҳисобланади. Ҳозирда бардошли криптографик алгоритмларни яратиш, уларни хавфсизлик нуқтаи назаридан баҳолаш масалаларига АҚШ, Россия Федерацияси, Исроил, Белгия, Жанубий Корея, Канада ва бошқа ривожланган давлатларда катта эътибор қаратилмоқда.

Жаҳонда ахборотни конфиденциаллигини таъминлашда криптографик шифрлаш алгоритмларидан фойдаланишга қаратилган усул ва алгоритмларни яратиш, бардошлилик ва самарадорлик нуқтаи назаридан такомиллаштириш ҳамда уларнинг хавфсизлигини криптотаҳлил усуллари ёрдамида баҳолашга оид кўплаб илмий тадқиқотлар олиб борилмоқда. Шу ўринда, ахборотни шифрлашда тезкор симметрик блокли алгоритмлардан фойдаланиш ва уларнинг криптобардошлигини таҳлиллашнинг янги ёндашувларига бағишланган илмий-амалий тадқиқотларга алоҳида эътибор қаратиш зарур ҳисобланади.

Республикамизда давлат ва хўжалик бошқарув органларида ахборотни ҳимоялашнинг криптографик механизмларини татбиқ этиш, хусусан, давлат хизматларидан масофадан фойдаланишда фойдаланувчиларнинг ҳақиқий-лигини текшириш ва маълумотлар конфиденциаллигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Ушбу вазифаларни амалга оширишда мавжуд миллий криптографик алгоритмларни хавфсизлик нуқтаи назаридан баҳолаш ва уларни такомиллаштириш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 14 мартдаги ПФ-5379-сон «Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари, 2007 йил 3 апрелдаги ПҚ-614-сон «Ўзбекистон Республикасида ахборотни

[1] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги Қарори ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги низомни тасдиқлаш ҳақида» ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда мазкур диссертация тадқиқоти маълум 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-амалий тадқиқотлар олиб бормоқдалар. Жаҳонда, B.Schneier, Y.Dodis, N.Ferguson, J.Kelsey, M.Matsui, L.Knudsen, N.Courtois, N.Harris, E.Biham, A.Shamir, J.L.Massey, Р.Олейников, О.Казимиров, Л.Бабенко, Е.Ищуковалар томонидан шифрлаш алгоритми ва бардошли криптографик акслантиришларни ишлаб чиқиш ҳамда уларни криптотаҳлиллаш бўйича илмий-тадқиқотлар олиб борилмоқда.

Республикамизда, П.Ф.Хасанов, М.Арипов, С.К.Ганиев, М.М.Каримов, Д.Е.Акбаров, Б.Ф.Абдурахимов, Г.У.Жураев, Ғ.Н.Туйчиев, А.Б.Сатторов, Х.П.Хасанов, Д.М.Курьязов ва бошқалар бошчилигидаги илмий жамоалар томонидан ахборотни криптографик ҳимоя усулларини ишлаб чиқиш, криптографик алгоритмларни баҳолаш масалалари билан боғлиқ тадқиқотлар олиб борилган.

Шу билан бир қаторда, O‘z DSt 1105:2009 симметрик шифрлаш алгоритмини такомиллаштириш ва интеграл, алгебраик криптотаҳлил усуллари ёрдамида баҳолаш масалаларига етарлича эътибор қаратилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот ишлари режасининг №Ф706-17 – «Ахборот тизимларида биометрик – криптографик технологиялар қўлланилишининг тадқиқи» (2017-2018) мавзусидаги лойиҳа доирасида бажарилган.

Тадқиқотнинг мақсади O‘z DSt 1105:2009 симметрик шифрлаш алгоритмини такомиллаштириш ҳамда унинг бардошлилигини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолашдан иборат.

Тадқиқотнинг вазифалари:

симметрик блокли шифрлаш алгоритмлари ва уларнинг бардошлигини баҳолаш усулларини таҳлиллаш;

O‘z DSt 1105:2009 симметрик шифрлаш алгоритмини бардошлигини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш;

тезкорлик ва хавфсизлик нуқтаи назаридан такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритми ва унинг дастурий воситасини ишлаб чиқиш;

такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг бардошлигини баҳолаш.

Тадқиқотнинг объекти сифатида симметрик шифрлаш алгоритми ҳамда криптотаҳлил жараёнлари олинган.

Тадқиқотнинг предметини O‘z DSt 1105:2009 симметрик шифрлаш алгоритмини такомиллаштириш ҳамда унинг бардошлилигини интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш усуллари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида амалий криптография ва криптотаҳлил усуллари, эҳтимоллар назарияси, қиёсий таққослаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

O‘z DSt 1105:2009 симметрик шифрлаш алгоритмининг бардошлиги интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳоланган;

ўрнига қўйиш ва аралаштириш акслантириш усулларида параметрларни статик танлаш орқали такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрлаш алгоритми ишлаб чиқилган;

такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрида фойдаланилган акслантиришлар асосида раунд калитларини ҳосил қилиш алгоритми ишлаб чиқилган;

такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрлаш алгоритмининг бардошлиги интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳоланган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

O‘z DSt 1105:2009 шифрлаш алгоритмини алгебраик ва интеграл криптотаҳлил усуллари ёрдамида баҳолаш имкониятини берувчи дастурий воситалар ишлаб чиқилган;

маълумотни конфиденциаллигини таъминлаш учун такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрлаш алгоритмининг дастурий воситаси ишлаб чиқилган;

турли узунликдаги шифрлаш калитлари асосида раунд калитларини ҳосил қилиш алгоритмининг дастурий воситаси ишлаб чиқилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги қатъий таққослаш усуллари орқали исботланган ва ўтказилган сонли тадқиқот натижалари билан тасдиқланган ҳамда криптографик алгоритмларни криптотаҳлил усулларидан олинган реал ҳамда тажрибавий таҳлиллар билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти симметрик блокли шифрларни интеграл ва алгебраик криптотаҳлил усуллари ёрдамида баҳолаш ҳамда таклиф этилган раунд калитларини генерациялаш алгоритмини замонавий симметрик блокли шифрларда қўллаш мумкинлиги билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти таклиф этилган раунд калити генератори ва такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрлаш алгоритмининг дастурий воситасидан маълумотларни шифрлашда фойдаланиш мумкинлиги билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Таклиф этилган раунд калитини генерациялаш усули ва такомиллаштирилган O‘z DSt 1105:2009 симметрик шифрлаш алгоритмининг дастурий воситаси бўйича олинган натижалар бўйича:

такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг дастурий воситаси ва криптотаҳлил натижалари «UNICON.UZ» ДУК га жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 1 апрелдаги №33-8/2358-сон маълумотномаси). Илмий тадқиқот натижасида такомиллаштирилган маълумотларни шифрлаш алгоритми миллий ҳимояланган электрон тизимларда маълумотлар конфиденциаллигини таъминлаш имконини берган;

ўрнига қўйиш ва аралаштириш акслантириш усулларидаги параметрларни статик танлаш, раунд калитларини бевосита генерациялаш асосида такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг дастурий воситаси Тошкент шаҳри «SSP Maroqand» кўп функцияли ахборот маркази унитар корхонасига жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 1 апрелдаги №33-8/2358-сон маълумотномаси). Такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг дастурий воситаси мижоз маълумотларини 300 Кбит/с тезликда шифрлаш имконини берган;

такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг дастурий воситаси, S блокларни генерациялашдаги ёндашув ва раунд калитларини генерациялаш алгоритми Мудофаа вазирлиги Ахборот – коммуникация технологиялари ва алоқа ҳарбий институти кафедрасида «Криптография усуллари» фани доирасида курсантлар учун ўқув жараёнида татбиқ этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2021 йил 1 апрелдаги №33-8/2358-сон маълумотномаси). Илмий тадқиқот натижасида такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритми мавжудига нисбатан 22 Кбайт/с га юқори тезликда шифрлаш имконини берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 2 та халқаро ва 10 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертация мавзуси бўйича жами 24 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 4 таси хорижий ва 5 таси республика журналларида нашр этилган ҳамда ЭҲМ учун яратилган 3 та дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 115 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 **«Симметрик блокли шифрлаш алгоритмларининг таҳлили»** деб номланган биринчи боби симметрик блокли шифрлаш алгоритмларининг криптографиядаги ўрни, қўлланилиш соҳалари ва уларни яратиш усулларига бағишланган. Шунингдек, симметрик блокли шифрлаш алгоритмларини криптотаҳлиллаш усуллари ва замононавий симметрик блокли шифрлаш алгоритмларининг криптотаҳлил натижалари баён қилинган.

Криптографик ҳимоя ахборотни кибержиноятчилар ёки қонуний қабул қилувчидан бошқа фойдаланувчилар томонидан фойдаланилишини олдини олиш билан шуғулланиб, сақланган, ишланаётган ва тармоқда узатилаётган ахборотни конфиденциаллигини, яхлитлигини таъминлаш ҳамда рад этишдан ҳимоялаш имкониятини беради.

Симметрик блокли шифрлаш алгоритмлари тезкор ва юқори бардошликка эгалиги боис, амалда кенг қўлланилиб, аксарият давлатлар мазкур соҳада ўзларининг стандарт алгоритмларига эга. Симметрик блокли шифрларни ички тузилишига кўра 5 та: ўрнига қўйиш – алмаштириш тармоқлари (Substitution Permutation Networks, SPN), Фейстель тармоғи (Feistel networks), қўшиш-айлантириш-XOR (Add-Rotate-XOR, ARX), чизиқсиз алоқали силжитиш регисторларига (non-linear feedback shift register, NLFSR) асосланган ва гибрид турларга ажратиш мумкин. Ҳозирда SPN ва Фейстель тармоғига асосланган кўплаб давлат стандартлари (O'z DSt 1105:2009, ГОСТ Р 28147-89, AES) мавжуд.

Симметрик блокли шифрлардан амалда кенг фойдаланиш ўз навбатида уларни хавфсизлик нуқтаи назаридан баҳолашни талаб этади. Симметрик блокли шифрларни криптотаҳлиллашнинг кенг тарқалган усуллари сифатида, чизиқли криптотаҳлил (linear cryptanalysis), дифференциал криптотаҳлил (differential cryptanalysis), чизиқли-дифференциал криптотаҳлил (linear-differential cryptanalysis), алгебраик криптотаҳлил (algebraic cryptanalysis), интеграл криптотаҳлил (integral cryptanalysis), мисол келтириш мумкин. Криптотаҳлил натижаси эса у талаб қилган *маълумот (data, D)*, *вақт (time, T)* ва *хотира (memory, M)* омиллари билан характерланади.

Ушбу омиллар бўйича аксарият замонавий симметрик блокли шифрлаш алгоритмлари таҳлил қилинган. Таҳлил натижалари алгоритмларни амалий

томондан заифлигини кўрсатмасада, унинг тузилиши ва акслантиришларидаги муҳим камчиликларни ошкор қилади. Бу эса янги симметрик блокли шифрларни яратиш учун муҳим ҳисобланади.

Бироқ, олиб борилган тадқиқотлар O'z DSt 1105:2009 симметрик блокли шифрлаш алгоритми юқорида келтирилган криптотаҳлил усуллари ёрдамида баҳоланмаганини кўрсатди. Шу сабабли кейинги бобда O'z DSt 1105:2009 шифрлаш алгоритмини алгебраик ва интеграл криптотаҳлил ёрдамида баҳолаш масаласи кўриб ўтилади.

Диссертациянинг **«O'z DSt 1105:2009 шифрлаш алгоритмининг криптобардошлигини алгебраик ва интеграл криптотаҳлил усуллари ёрдамида баҳолаш»** деб номланган иккинчи бобида O'z DSt 1105:2009 шифрлаш алгоритмининг алгебраик ва интеграл криптотаҳлили амалга оширилган.

O'z DSt 1105:2009 шифрлаш алгоритми симметрик блокли шифрлар турига мансуб бўлиб, SPN тармоғига асосланади. Алгоритмда шифрлаш блоки узунлиги 256 бит, шифрлаш калитлари 256 ёки 512 бит бўлиши мумкин. Алгоритм асосан икки қисмдан калитларни генерациялаш ва шифрлаш/расшифровкалаш жараёнларидан ташкил топган. Калитларни генерациялаш босқичида шифрлаш калити ва функциональ калитдан фойдаланиб раунд калитларини ва S блокларни ҳосил қилиш босқичлари бажарилади. Бу босқичлар қуйидаги $ShaklSeansKalitBayt()$, $ShaklSeansKalit()$, $ShaklBosqichKalit()$ функцияларини кетма-кет бажариш орқали амалга оширилади.

Шунингдек, алгоритм таркибида тўртта акслантириш функцияларидан фойдаланилган. Булар $Qo'shBosqishKalit\ ()\rightarrow X$, $Aralash()\rightarrow A$, $Sur()\rightarrow S$ ва $BaytAlmash()\rightarrow B$ акслантишлари. Алгоритмда фойдаланилган $Aralash()$ ва $BaytAlmash()$ акслантиришлари асосий чизиқсиз акслантиришлар ҳисобланиб, алгоритм криптобардошлигини таъминлашда муҳим ҳисобланади. Шунинг учун, криптотаҳлиллар асосан ушбу акслантиришларга нисбатан амалга оширилади. Ўтказилган алгебраик криптотаҳлилда $BaytAlmash()$ акслантиришида фойдаланиладиган жадвалларга нисбатан тузилган тенгламалар системаларининг хусусиятлари қуйидаги 1–жадвалда келтирилган.

1 – жадвал

Турли калитлардан ҳосил қилинган $BaytAlmash()$ жадвалларига тузилган тенгламалар системалари параметрлари

№	Чизиқсизлиги	Алгебраик иммунитети	Тенгламалар сони	№	Чизиқсизлиги	Алгебраик иммунитети	Тенгламалар сони
1.	92	3	441	6.	90	3	441
2.	90	3	441	7.	92	3	441
3.	90	3	441	8.	94	3	441
4.	94	3	441	9.	94	3	441
5.	94	3	441	10.	70	3	441

Натижалар 4×4 ўлчамли 10 та махсус тузилмали диаматрицаларни таҳлил қилишдан олинган. Бунда, ҳосил қилинган алгебраик тенгламалар

системаларининг энг кичик даражаси Deg=7 га тенг бўлади. Ҳосил қилинган бирҳадларнинг максимал сони 17742 тани ташкил этди (2-жадвал).

2– жадвал

Турли калитлардан ҳосил қилинган диаматрицалар учун диагонал элементларни ифодаловчи тенгламалар системалари параметрлари

№	Тенгламалар даражаси (та)								Бирҳадлар сони
	Deg=1	Deg=2	Deg=3	Deg=4	Deg=5	Deg=6	Deg=7	Deg=8	
1.	4	4	4	4	4	4	4	4	14993
2.	4	6	2	6	2	4	4	4	13395
3.	4	4	4	4	4	4	4	4	14993
4.	4	6	2	5	3	4	4	4	17674
5.	4	4	4	4	4	4	4	4	4784
6.	4	8	0	7	1	7	1	4	7036
7.	4	4	4	4	4	4	4	4	14993
8.	4	7	1	7	2	6	1	4	17742
9.	4	4	9	3	3	3	3	3	3674
10.	4	5	3	4	4	4	4	4	15240

Бундан ташқари, O‘z DSt 1105:2009 шифрлаш алгоритмида ишлатилган тўртта акслантиришлар ўрнини алмаштириш алгоритмнинг умумий криптографик баҳосига таъсир қилиши аниқланди. Тўртта акслантириш функциясининг жами ўрин алшаштиришларининг сони 24 та бўлиб, ҳолатларнинг ҳар бири учун алгебраик криптотаҳлил ўтказилди ва қуйидаги натижалар олинди (3-жадвал).

3-жадвал

O‘z DSt 1105:2009 шифрлаш алгоритми акслантиришлари ўринларини алмаштирилган ҳолатлари учун тузилган тенгламалар кўрсаттичлари

	Акслантиришлар тартиби	1 раунд			I	II	2 раунд			I	II
		TS	Deg	NS			TS	Deg	NS		
1	2	3	4	5	6	7	8	9	10	11	12
1.	XASB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
2.	XABS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
3.	XBSA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
4.	XBAS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
5.	XSBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
6.	XSAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
7.	AXSB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
8.	AXBS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
9.	ABSX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
10.	ABXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
11.	ASBX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
12.	ASXB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
13.	SAXB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
14.	SABX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
15.	SBXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
16.	SBAX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
17.	SXBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
18.	SXAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
19.	BASX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
20.	BAXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}

1	2	3	4	5	6	7	8	9	10	11	12
21.	BXSA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
22.	BXAS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
23.	BSXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
24.	BSAX	256	1	2^{8}	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}

Изоҳ:TS – тенгламалар сони, Deg – даражаси, NS – номаълумлар сони, I – TC ни ечиш мураккаблиги ($\approx O(NS)^3$), II – TC ни сақлаш учун зарур хотира ҳажми (байт)

Ушбу таҳлил натижаларидан хулоса қилиш мумкинки, O‘z DSt 1105:2009 шифрлаш алгоритмини алгебраик криптотаҳлил усули ёрдамида баҳоланганда шаклланадиган тенгламалар системасини иккинчи раунддан кейин сақлаш учун 2^{73} байт хотира талаб қилинади. Ушбу талаб қилинадиган хотира ҳажмини таъминлаш имкониятининг мавжуд эмаслиги алгоритм иккинчи раунддан сўнг алгебраик криптотаҳлил усулига бардошли.

Шунингдек, O‘z DSt 1105:2009 шифрлаш алгоритми интеграл криптотаҳлил усули ёрдамида баҳоланди. Тадқиқот натижаси алгоритмда фойдаланилган *Aralash()* акслантириши унинг интеграл криптотаҳлилга бардошлилигини таъминлашини кўрсатди. Қуйида тўрт раундли O‘z DSt 1105:2009 алгоритмига интеграл криптотаҳлил усулини қўллаб сўнги раунд калитини топиш натижалари 1-расмда келтирилган.

Бу ерда: А – актив (A_i– агар ташкил этувчилари турли тартибда жойлашган бўлса) ёки П – пассив ёки Д – аралаш ($Д_0$– баланслашган бўлса, $Д_1$– баланслашмаган бўлса).

Таҳлил натижаси 2-раунд сўнгидаги *BaytAlmash*() акслантиришининг хоссаларига мувофиқ шу раунд калитининг K_1^4, K_5^4, K_{14}^4, K_{15}^4, K_{20}^4, K_{21}^4, K_{27}^4, K_{30}^4, K_{31}^4 қийматлари ноаниқлигини кўрсатди. Ушбу калит байтларини тўлиқ танлаш усули ёрдамида топиш 2^{72} та ҳисоблашни талаб қилади.

Диссертация ишининг **«Такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмини ишлаб чиқиш»** номли учинчи боби O‘z DSt 1105:2009 шифрлаш алгоритмининг *BaytAlmash()* акслантириши учун S жадваллар, *Aralash()* акслантириши учун диаматрицаларни статик тарзда танлаш масалаларига бағишланган. Бундан ташқари, раунд калитларини боғлиқсиз равишда ҳосил қилиш алгоритми ишлаб чиқилган ва улар асосида DSt 1105:2009 шифрлаш алгоритми такомиллаштирилган.

O‘z DSt 1105:2009 шифрлаш алгоритмида *BaytAlmash()* акслантириши учун S жадваллар, *Aralash()* акслантириши учун диаматрицалар киритилган шифрлаш ва функционал калитлар орқали динамик ҳосил қилинади. Ушбу динамик ўзгарувчиларни статик танлаш алгоритмга нисбатан аниқ криптографик баҳо бериш имконини яратади. Бундан ташқари, алгоритмда ҳар сафар шифрлашдан олдин динамик ўзгарувчиларни генерациялаш унинг тезкорлигини камайтиради.

O‘z DSt 1105:2009 шифрлаш алгоритми учун S жадвалларни статик ҳосил қилишда унинг криптографик талабларга жавоб беришини текшириш лозим. Шунинг учун *BaytAlmash*() акслантиришидаги иккита S жадвал ўрнига қуйидаги параметрли жадваллардан фойдаланиш талаби қўйилди:

1. $N(S)$ кўрсаткичи максимал ва δ кўрсаткичи минимал бўлган 8×8 ўлчамли жадвал (S_1);

2. $AI(S)$ кўрсаткичи максимал бўлган 8×8 ўлчамли жадвал (S_2).

1-раунд:

Qo`shBosqichKalit()							
A	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П

Aralash()							
A	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П
П	П	П	П	П	П	П	П

Sur()							
П	П	П	A	A	П	П	П
П	A	A	П	П	П	П	П
A	П	П	П	A	П	П	П
П	П	П	П	П	П	A	П

BaytAlmash()							
П	П	П	A	A	П	П	П
П	A	A	П	П	П	П	П
A	П	П	П	A	П	П	П
П	П	П	П	П	П	A	П

2-раунд:

Qo`shBosqichKalit()							
П	П	П	A	A	П	П	П
П	A	A	П	П	П	П	П
A	П	П	П	A	П	П	П
П	П	П	П	П	П	A	П

Aralash()							
A_1	$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_0$
$Д_0$	A_1	$Д_0$	A_1	A_1	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	A_1	A_1	A_1

Sur()							
$Д_0$	A_1	A_1	A_1	$Д_0$	A_1	A_1	A_1
A_1	A_1	A_1	A_1	A_1	$Д_0$	$Д_0$	A_1
A_1	A_1	A_1	$Д_0$	$Д_0$	A_1	A_1	A_1
A_1	A_1	$Д_0$	A_1	A_1	$Д_0$	$Д_0$	A_1

BaytAlmash()							
$Д_1$	$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_0$	$Д_0$	$Д_0$
$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$
$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$	$Д_0$	$Д_0$
$Д_0$	$Д_0$	$Д_1$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$

3-раунд:

Qo`shBosqichKalit()							
$Д_1$	$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_0$	$Д_0$	$Д_0$
$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$
$Д_0$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$	$Д_0$	$Д_0$
$Д_0$	$Д_0$	$Д_1$	$Д_0$	$Д_0$	$Д_1$	$Д_1$	$Д_0$

Aralash()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

Sur()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

BaytAlmash()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

4-раунд:

Qo`shBosqichKalit()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

Aralash()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

Sur()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

BaytAlmash()							
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$
$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$	$Д_1$

1-расм. O‘z DSt 1105:2009 шифрлаш алгоритмининг интеграл криптотаҳлили

Биринчи талабни қаноатлантирувчи S жадвални яратишда AES стандартида фойдаланилган ёндашувдан фойдаланилди.

$$y = (Ax^{-1} \oplus c) mod\ m(x)$$

Бу ерда, y – чиқувчи байт, A – аффин матрицаси, x^{-1} – кирувчи байтнинг инверси, $c = 0x63$ – ўзгармас қўшилувчи.

Юқоридаги қоидалар асосида ҳосил қилинган S_1 жадвал криптографик талабларга баҳоланганда қуйидаги натижалар олинди (4-жадвал).

4-жадвал

Генерацияланган S_1 ва S_2 жадвалнинг баҳолаш натижалари

Баҳолаш омиллари		Қиймати (S_1)	Қиймати (S_2)
Балансланганлик		True	True
Регулярлик		True	True
Чизиқсизлик, $N(S)$		112	104
Корреляцион иммунитет, (CI)		0	0
Минимал даража, deg		7	7
Айирма матрица жадвалидаги максимал қиймат, δ		4	8
$D(S)$		133120	194944
Қатъий лавин самарадорлик, SAC		False	False
Алгебраик иммунитет	AI(S)	2	3
	TS(S)	39	441

Ушбу натижаларнинг эътиборли томони, яратилган S_1 жадвалнинг чизиқсизлик даражаси $N(S)$ максимал ва ва δ кўрсаткичи минимал бўлиб, бу алгоритмнинг чизиқли, дифференцал ва чизиқли-дифференциал криптотаҳлилга бардошли бўлишини таъминлайди. Бошқа томондан, алгоритм алгебраик таҳлилга бардошли бўлиши ҳам талаб этилади (бу икки талаб бир вақтда бажарилмайди). Шу боис, алгоритмдаги иккинчи – S_2 жадвални ҳосил қилишда унинг юқори алгебраик иммунитетга эга бўлишига эътибор қаратилади.

Шунинг учун яратиладиган S_2 жадвални учун қуйидаги тасдиқ белгилаб олинди:

1-тасдиқ. *AI* параметр қиймати максимал бўлган оптимал S(8×8) – жадвал учун $AI(S) = 3, N_{TS} = 441$ ва $N(S) \geq 104$ ўринли.

Юқорида келтирилган тасдиққа мос келувчи S жадвалларни яратишда қуйидаги икки босқичдан иборат бўлган ишлар амалга оширилган:

1. Чизиқсизлик даражаси юқори ($N(S) = 112$) бўлган S(8×8) жадвални олиш.

2. S(8×8) жадвални тасодифий N та элементини ўзаро ўрнини алмаштириш.

N қиймати 22 га тенг бўлган ҳол учун тажрибалар олиб борилиб, 4-жадвалда келтирилган криптографик хусусиятларга эга S_2 жадвал ҳосил қилинди.

S_2 жадвалнинг алгебраик иммунитети юқори бўлиб, ундан алгоритм таркибида фойдаланиш унинг алгебраик криптотаҳлилга бардошли бўлишини таъминлайди.

O'z DSt 1105:2009 шифрлаш алгоритми таркибида функционал калитдан динамик ҳосил қилинадиган кейинги элемент бу махсус тузилмали диаматрицалар ҳисобланади. Ушбу махсус тузилмали диаматрицаларни алгоритм таркибида статик фойдаланиш учун қуйидаги кетма-кетликдаги ишлар амалга оширилди:

1. Тасодифий танланган калитлар асосида K_1 ва K_2 диаматрицаларни ҳосил қилиш.

2. Ҳар бир K_1 ва K_2 диматрицалар жуфти учун бир битнинг ўзгаришини ҳар бир раундда неча битга таъсир қилишини аниқлаш.

Тажрибада 200 та турли K_1 ва K_2 диаматрицалар жуфтлари ҳосил қилинди. Ҳар бир диаматрицалар жуфтларининг ҳар раунддан кейинги тарқатиш кўрсаткичлари (SAC - қатъий лавин самарадорлик) аниқланди. Олинган натижалар O'z DSt 1105:2009 шифрлаш алгоритмини барча ҳосил қилинган диаматрицалар жуфтлари учун 3-раунддан сўнг максимал тарқатиш даражасига эришишини кўрсатди. Бошқа томондан, ҳосил қилинган K_1 ва K_2 диматрицалар жуфтларидан бирини статик равишда фойдаланиш мумкинлигини ҳам кўрсатди. Ҳосил қилинган диматрицалар жуфтлари орасидан қуйидаги икки диматрицалар жуфти статик равишда фойдаланиш учун танлаб олинди.

$$K_1 = \begin{vmatrix} 149 & 157 & 87 & 182 \\ 92 & 149 & 92 & 92 \\ 13 & 77 & 149 & 13 \\ 157 & 68 & 184 & 149 \end{vmatrix} \qquad K_2 = \begin{vmatrix} 157 & 150 & 197 & 66 \\ 52 & 157 & 52 & 52 \\ 86 & 233 & 157 & 86 \\ 184 & 241 & 69 & 157 \end{vmatrix}$$

Шифрлаш ва расшифровкалаш жараёни учун ушбу икки диаматрицаларга тескари бўлган диаматрицалар аниқланади ва улардан фойдаланилади.

Одатда раунд калитларини ишлаб чиқиш олдинги раунд калитидан фойдаланишга асосланилади. Масалан, AES ва O'z DSt 1105:2009 шифрлаш алгоритмларида. Бунга кўра, биринчи раунд калити кейинги раунд калитини ҳосил қилишда ишлатилади ва ҳ. Бу эса ўз навбатида раунд калитларини сақлаб туриш учун юқори хотира ҳажмини талаб этади. Хусусан, раунд калитларидан тескари фойдаланишга асосланган расшифровкалаш жараёнида дастлаб калитларни генерациялаш ва уларни сақлаш талаб этилади. Шу сабабли, мавжуд муаммоларни олдини олувчи ва ҳар бир раунд калитларини мустақил равишда генерациялаш имкониятига эга бўлган $\phi()$ – функцияни шакллантириш талаб этилади:

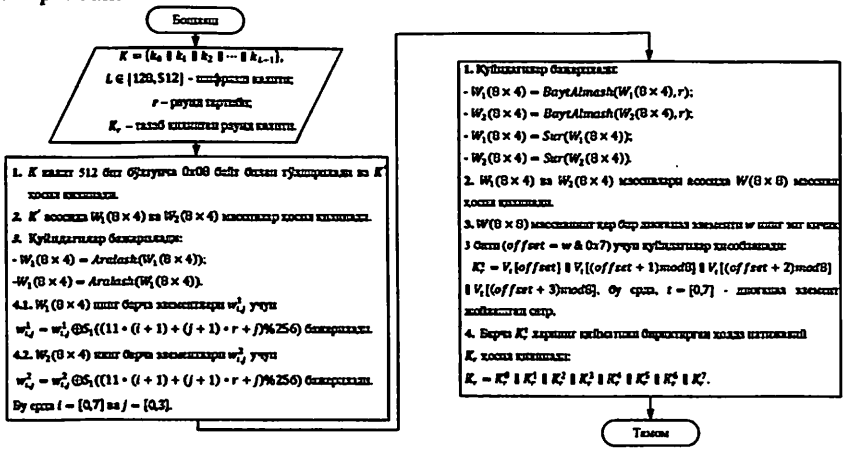
$$K_i = \phi(K, i).$$

Бу ерда, K – шифрлаш калити, i – раунд сони ва K_i эса i – раунд калити. Бошқача айтганда, ҳар бир раунд калити шифрлаш калити ва рауд сони асосида ҳосил қилинади. Бундан ташқари, ишлаб чиқилаётган раунд калит генератори қуйидаги талабларга жавоб бериши талаб қилинсин:

- раунд калитидан шифрлаш калитини ҳисоблашнинг имконсизлиги (бир томонламалик);
- турли узунликдаги шифрлаш калитларини қабул қилиши ва чиқишда ҳам талаб этилган узунликдаги раунд калитларини ҳосил қилиш.

Юқорида келтирилган талаблар ва тавсиялар асосида такомиллаштирилган O'z DSt 1105:2009 шифрлаш алгоритми учун раунд калитини генерациялаш алгоритми ишлаб чиқилди (2-расм).

Ишлаб чиқилган калит генераторидан ҳосил бўлган псевдотасодифий кетма-кетликларни баҳолаш NIST статистик тестлар тўплами ёрдамида амалга оширилди. Тестлашда дастлабки киритилувчи шифрлаш калитининг узунлиги 128, 192, 256, 512 битга тенг бўлган тасодифий танланган ҳамда узунлиги 128 битли заиф калитлар (00, FF, 01, E1 ва EF байтлардан иборат бўлган) киритилган ҳолат учун амалга оширилди. Тестлаш натижаси 6-жадвалда келтирилган.



2-расм. Раунд калит генерацияси алгоритмининг блок схемаси (256 битли раунд калити учун)

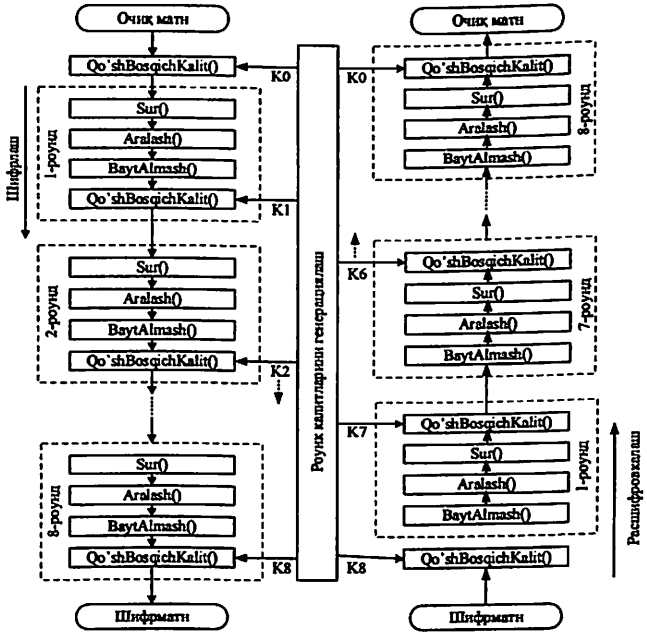
6-жадвал

Псевдотасодифий кетма-кетликларнинг статистик тестлаш натижалари

№	Дастлабки калит узунлиги ва тасодифийлик даражаси	Намуналар				
		1	2	3	4	5
1.	128 бит ва тасодифий	15/16	15/16	15/16	15/16	14/16
2.	192 бит ва тасодифий	15/16	15/16	15/16	15/16	15/16
3.	256 бит ва тасодифий	15/16	15/16	15/16	15/16	15/16
4.	512 бит ва тасодифий	15/16	15/16	14/16	14/16	15/16
5.	128 бит ва заиф (0x00, 0xFF, 0x01, 0xE1 ва 0xEF иборат бўлган)	15/16	13/16	13/16	15/16	15/16

Олинган тестлаш натижалари ишлаб чиқилган калит генераторини турли узунликдаги ва тасодифийлик даражаси турлича бўлган шифрлаш калитлари учун бардошли бўлган раунд калитларини ҳосил қилишини кўрсатди.

Юқорида келтирилган акслантиришлар ва раунда функциялари асосида такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг шифрлаш ва расшифровкалаш кетма-кетлиги 3-расмда акс эттирилган.



3-расм. Такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмида шифрлаш ва расшифровкалаш кетма-кетлиги

Диссертациянинг **«Такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмини баҳолаш»** номли тўртинчи боби такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмини тезлик ва бардошлилик хусусиятлари асосида баҳолашга бағишланган.

Такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмида мавжудидаги акслантириш функцияларининг ўзгармаган. Юқорида акслантириш функциялари тартибини ўзгартирилиши шифрлаш алгоритмининг бардошлигига таъсир қилиши айтиб ўтилган эди. Тўртта акслантириш функциясининг барча вариантларидан қатъий лавин самарадорлиги бажарилган 6 та ҳолати учун интеграл таҳлил натижалари қуйидаги 7-жадвалда келтирилган.

7-жадвал

Акслантириш функцияларининг турли тартибн учун 2-раунддан сўнг чиқиш байтларига таъсири

№	Акслантириш тартиби	Таъсирн
1.	B→Q→S→A	12
2.	Q→S→B→A	15
3.	Q→S→A→B	12
4.	S→Q→A→B	15
5.	S→A→B→Q	15
6.	S→A→Q→B	15

MUHAMMAD AL... NOMIDAGI TOSHKENT ... AXBOROT TEXNOLOGIYALARI UNIVERSITETI
A/2650
AXBOROT-RESURS MARKAZI

Ушбу натижалар такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг 4 раундли варианти учун ҳисобланган бўлиб, мазкур ҳолатда очиқ матнлар сони 2^8 тани ташкил этган.

Масалан, такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмининг S→A→B→Q акслантириш тартибили варианти учун 2-раунддан сўнг 12 байт элементлари номаълум бўлганлигини қуйидагича асосланади.

Ҳолат массивининг бир байт элементи актив бўладиган тўплам танланади ва унинг S→A→B→Q хар раундан чиқиш қийматларининг баланслашганлик хусусиятлари кузатилади. Танлаб олинган очиқ матнларга мос шифр матнлар тўплами T_i мавжуд бўлганда, дешифрлаш жараёни кетма-кетлиги қуйидагича:

$$C_i = Sur(Aralash(BaytAlmash(Qo'shBosqichKalit(T_i, K^4))))$$

Бу ерда, C_i массив тўртинчи раунд киришидаги ҳолатни ифодалайди. K^4 калитнинг K_q^4 $(1 \le q \le 32)$ байтлари қабул қилиши мумкин бўлган барча (0 дан 255 гача) қийматларида C_i массивни учинчи раунддаги акслантиришлардан ўтказилади:

$$R_{iq} = Sur\left(Aralash\left(BaytAlmash(C_i)\right)\right)$$

Шундан сўнг, R_{iq} қийматларнинг *XOR* йиғиндиси ҳисобланади:

$$XOR = R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus R_{mq}$$

Агар $XOR = 0$ га тенг бўлса, K_q^4 $(1 \le q \le 32)$ раунд калити номзод калитлар рўйхатига қўшилади.

Юқоридаги таҳлил натижаларидан келиб чиқиб шуни айтиш мумкинки, S→A→B→Q тартибли акслантиришга эга 4 раундли O‘z DSt 1105:2009 шифрлаш алгоритми асосида такомиллаштирилган шифрлаш алгоритмига интеграл криптотаҳлил усулини қўллаб, танлаб олинган 2^8 та очиқ матнлар асосида 2-раунд сўнгидаги *BaytAlmash()* акслантиришининг хоссаларига мувофиқ шу раунд чиқишидаги калитнинг K_2^4, K_4^4, K_5^4, K_7^4, K_9^4, K_{10}^4, K_{11}^4, K_{12}^4, K_{14}^4, K_{17}^4, K_{19}^4, K_{20}^4, K_{21}^4, K_{22}^4, K_{25}^4, K_{28}^4, K_{29}^4, K_{30}^4, K_{31}^4, K_{32}^4 байтларини (жами 160 бит) топиш мумкин. 2-раунд сўнгидаги *BaytAlmash()* акслантиришининг хоссаларига мувофиқ тўртинчи раунддаги калитнинг қолган K_1^4, K_3^4, K_6^4, K_8^4, K_{13}^4, K_{15}^4, K_{16}^4, K_{18}^4, K_{23}^4, K_{23}^4, K_{24}^4, K_{26}^4, K_{27}^4 байтларини тўлиқ танлаш усулидаги жами вариантлар сони 2^{96} га тенг бўлади.

Бундан ташқари, такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмини криптографик баҳолаш учун алгебраик криптотаҳлил усули қўлланилди. Ўтказилган экспериментлар O‘z DSt 1105:2009 шифрлаш алгоритмидаги *Aralash()* ҳамда *BaytAlmash()* акслантиришлари алгоритмни ифодаловчи тенгламалар системаси даражаси ва номаълумлар сонига таъсир этувчи асосий акслантиришлар эканлигини кўрсатди.

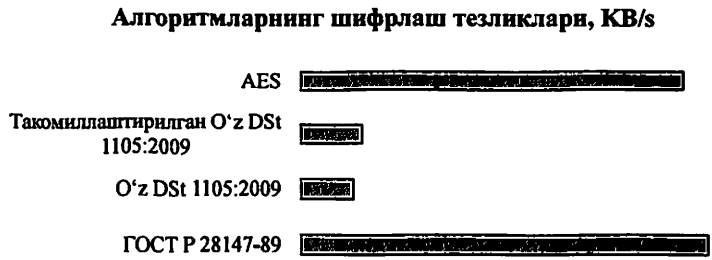
BaytAlmash() акслантириши учун қўлланилган алгебраик криптотаҳлил такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмида фойдаланилган S_1 ва S_2 жадваллар учун ўтказилди. Унга кўра S_1 жадвал учун

2 ва 3 - даражали тенгламалар сони мос ҳолда 39 ва 471 тани, S_2 жадвал учун 3 - даражали тенгламалар сони 441 тага тенг бўлган.

Шунингдек, такомиллиштирилган шифрлаш алгоритмининг *Aralash()* акслантиришида фойдаланилган диаматрицаларнинг диагонал элементлари учун алгебраик криптотаҳлил ўтказилди. Олинган натижага кўра шифрлашда ишлатиладиган K_1, K_{2t} махсус тузилмали диаматрицаларга кириш ва чиқиш битларининг боғлиқлиги тенгламаларида бирҳадларнинг умумий сони 14993 тани ташкил қилган.

Хулоса қилиб айтганда, ўтказилган экспериментлар натижаларидан келиб чиқиб, раунд калитларини мустақил равишда генерациялаш алгоритмни алгебраик криптотаҳлилга бардошлигини 2-раунддан сўнг икки бараварга оширишини кўриш мумкин.

Бундан ташқари, такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритми тезкорлик нуқтаи назаридан ҳам баҳоланди. Бунда, мавжуд ва такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмларининг дастурий воситалари ишлаб чиқилди. Шунингдек, ГОСТ Р 28147-89 ва AES шифрлаш алгоритмларининг C# дастурлаш тилидаги кутубхонасидан фойдаланилди. Шифрлаш тезликларини юқори аниқликда олиш учун .NET муҳити дастурий воситаларига мўлжалланган ANTS Performance Profiler дастурий воситасидан фойдаланилди (4-расм).



4-расм. Алгоритмларнинг маълумотни шифрлаш тезликлари

Мавжуд ва такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритмларининг маълумотларни ишлашда паст тезлик қайт этганининг боиси, *Aralash()* акслантиришдаги махсус тузилмали диаматрицаларни кўпайтириш амалидан фойдаланилгани ҳисобланади. Шунга қарамай такомиллаштирилган O‘z DSt 1105:2009 шифрлаш алгоритми мавжудига нисбатан 22 Кбайт/с юқори тезликни қайт этди.

ХУЛОСА

«Симметрик шифрлаш алгоритмини такомиллаштириш ва криптотаҳлил усуллари ёрдамида баҳолаш» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Симметрик блокли шифрлаш алгоритмлари ва уларнинг бардошлигини баҳолаш усуллари таҳлил қилинди. Таҳлил натижасида замонавий симметрик блокли шифрларнинг бардошлигини баҳолашда чизиқли, дифференциал, интеграл ва алгебраик криптотаҳлил усулларидан кенг фойдаланилиши аниқланди.

2. O'z DSt 1105:2009 шифрлаш алгоритми таркибий қисми ва тузилиши бўйича таҳлил қилинди. O'z DSt 1105:2009 шифрлаш алгоритмидаги *BaytAlmash()* ва *Aralash()* акслантиришларидаги жадваллар, диаматрицалар сеанс калити асосида динамик тарзда ҳосил қилиниши алгоритмни аниқ баҳолашга имкон бермаслиги аниқланди.

3. O'z DSt 1105:2009 шифрлаш алгоритмининг бардошлиги алгебраик криптотаҳлил усуллари ёрдамида баҳоланди. Криптотаҳлил натижаси 2-раунд учун калитни топишда 2^{73} байт хотира кераклигини кўрсатгани боис, МША алгебраик криптотаҳлилга бардошли.

4. O'z DSt 1105:2009 шифрлаш алгоритмининг бардошлиги интеграл криптотаҳлил усуллари ёрдамида баҳоланди. Криптотаҳлил натижаси 2-раунд BaytAlmash() акслантиришидан кейинги шифрлаш калитини топишда 2^{72} та амал бажариш зарурлигини кўрсатди.

5. Статик бўлган юқори чизиқсизлик даражасига эга S_1 ва юқори алгебраик иммунитетга эга S_2 жадваллар асосида O'z DSt 1105:2009 шифрлаш алгоритмидаги *BaytAlmash()* акслантириши, қатъий лавин самарадорлигини таъминловчи статик 4×4 ўлчамли махсус тузилмали диаматрицалар асосида *Aralash()* акслантириши такомиллаштирилди. Натижада алгоритмни аниқ баҳолаш имконияти яратилди.

6. Раунд калитларини бир бирига боғлиқсиз генерациялаш алгоритми ишлаб чиқилди. Ишлаб чиқилган алгоритм NIST статистик тестлар тўплами асосида баҳоланганда 92% тасодифийлик даражасини қайд этди.

7. Такомиллаштирилган O'z DSt 1105:2009 шифрлаш алгоритми алгебраик криптотаҳлил усули ёрдамида баҳоланди. Таҳлил натижасида раунд калитларини мустақил равишда генерациялаш алгоритмни алгебраик криптотаҳлилга бардошлигини 2-раунддан сўнг икки бараварга ошириши аниқланди.

8. Такомиллаштирилган O'z DSt 1105:2009 шифрлаш алгоритми интеграл криптотаҳлил усули ёрдамида баҳоланди. Таҳлил натижасида раунд функцияси акслантиришларини турли тартибларда фойдаланиш алгоритмни интеграл криптотаҳлилга бардошлигига таъсир этиши аниқланди.

9. Такомиллаштирилган O'z DSt 1105:2009 шифрлаш алгоритмининг дастурий воситаси ишлаб чиқилди. Таҳлил натижасида махсус тузилмали диаматрицалардан ва S жадваллардан статик равишда фойдаланиш алгоритмнинг тезкорлигини ошириши аниқланди.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.01
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

АЛЛАНОВ ОРИФ МЕНГЛИМУРАТОВИЧ

СОВЕРШЕНСТВОВАНИЕ АЛГОРИТМА СИММЕТРИЧНОГО ШИФРОВАНИЯ И ОЦЕНКА С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ КРИПТОАНАЛИЗА

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

Ташкент-2021

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2021.2.PhD/T1940.

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице научного совета (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физика-математических наук, профессор
Официальные оппоненты:	**Жураев Гайрат Умарович** доктор физика-математических наук, доцент
	Юсупов Боходир Караматович доктора философии по техническим наукам (PhD)
Ведущая организация:	**«UNICON.UZ» - центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «__» _____2021 года в __ часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №___). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «___» _____ 2021 года.
(протокол рассылки №__ от «___» _____ 2021 года.)

Р.Х. Хамдамов
Председатель научного совета по присуждению ученых степеней, доктор технических наук, профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению ученых степеней, доктор технических наук, доцент

С.К.Ганиев
Председатель научного семинара при научном совете по присуждению ученых степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. При решении вопросов защиты информации во всем мире криптографическая защита занимает лидирующие позиции по своей высокой надежности защиты с гарантиями и ведущими приоритетами. В частности, согласно данным, предоставленным компанией Accenture, «в 2019 году организации сэкономили 0,85 миллиона долларов США в результате использования механизмов криптографической защиты»[3]. Поскольку криптографическая защита играет важную роль в обеспечении конфиденциальности, целостности характеристик информации и защите от отбраковки, оценка стойкости криптографических алгоритмов является одним из актуальных вопросов современности. В настоящее время в США, Российской Федерации, Израиле, Бельгии, Южной Корее, Канаде и других развитых странах уделяется большое внимание разработке надежных криптографических алгоритмов и их оценке с точки зрения безопасности.

В мире проводится множество научных исследований касательно разработки методов и алгоритмов использования алгоритмов криптографического шифрования для обеспечения конфиденциальности информации, улучшения с точки зрения стойкости и эффективности, а также оценки их безопасности методами криптоанализа. В связи с этим необходимо уделить особое внимание научно-практическим исследованиям по использованию оперативных симметричных блочных алгоритмов при шифровании информации и новым подходам к анализу их криптостойкости.

В нашей республике органами государственного и хозяйственного управления предпринимаются широкомасштабные меры, направленные на внедрение криптографических механизмов защиты информации, в частности, проверка подлинности пользователей и обеспечение конфиденциальности данных при дистанционном пользовании государственными услугами. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[4]. При выполнении этих задач одной из важных задач является оценка и совершенствование существующих национальных криптографических алгоритмов с точки зрения безопасности.

Данное диссертационное исследование, в определенной степени вносит вклад в выполнение задач, предусмотренных Указами Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5379 от 14 марта 2018 года «О мерах по совершенствованию системы государственной безопасности Республики Узбекистан», №ПП-614 от 3 апреля

[3] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[4] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2021.2.PhD/T1940.

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице научного совета (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физика-математических наук, профессор
Официальные оппоненты:	**Жураев Гайрат Умарович** доктор физика-математических наук, доцент
	Юсупов Боходир Караматович доктора философии по техническим наукам (PhD)
Ведущая организация:	**«UNICON.UZ» - центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «__» _____2021 года в __ часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №___). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «___» _____ 2021 года.
(протокол рассылки №__ от «___» _____ 2021 года.)

Р.Х. Хамдамов
Председатель научного совета по присуждению ученых степеней, доктор технических наук, профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению ученых степеней, доктор технических наук, доцент

С.К.Ганиев
Председатель научного семинара при научном совете по присуждению ученых степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. При решении вопросов защиты информации во всем мире криптографическая защита занимает лидирующие позиции по своей высокой надежности защиты с гарантиями и ведущими приоритетами. В частности, согласно данным, предоставленным компанией Accenture, «в 2019 году организации сэкономили 0,85 миллиона долларов США в результате использования механизмов криптографической защиты»[3]. Поскольку криптографическая защита играет важную роль в обеспечении конфиденциальности, целостности характеристик информации и защите от отбраковки, оценка стойкости криптографических алгоритмов является одним из актуальных вопросов современности. В настоящее время в США, Российской Федерации, Израиле, Бельгии, Южной Корее, Канаде и других развитых странах уделяется большое внимание разработке надежных криптографических алгоритмов и их оценке с точки зрения безопасности.

В мире проводится множество научных исследований касательно разработки методов и алгоритмов использования алгоритмов криптографического шифрования для обеспечения конфиденциальности информации, улучшения с точки зрения стойкости и эффективности, а также оценки их безопасности методами криптоанализа. В связи с этим необходимо уделить особое внимание научно-практическим исследованиям по использованию оперативных симметричных блочных алгоритмов при шифровании информации и новым подходам к анализу их криптостойкости.

В нашей республике органами государственного и хозяйственного управления предпринимаются широкомасштабные меры, направленные на внедрение криптографических механизмов защиты информации, в частности, проверка подлинности пользователей и обеспечение конфиденциальности данных при дистанционном пользовании государственными услугами. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[4]. При выполнении этих задач одной из важных задач является оценка и совершенствование существующих национальных криптографических алгоритмов с точки зрения безопасности.

Данное диссертационное исследование, в определенной степени вносит вклад в выполнение задач, предусмотренных Указами Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5379 от 14 марта 2018 года «О мерах по совершенствованию системы государственной безопасности Республики Узбекистан», №ПП-614 от 3 апреля

---

[3] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[4] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

2007 года «О мерах по организации криптографической защиты информации в Республике Узбекистан» и Постановлением Кабинета Министров Республики Узбекистан №ПКМ-242 от 21 ноября 2007 года «Об утверждении положения о лицензировании деятельности по проектированию, разработке, производству, реализации, ремонту и использованию средств криптографической защиты информации» и другими нормативно-правовыми документами, принятыми в данной сфере.

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 проводят исследования по криптоанализу симметричных блочных алгоритмов шифрования и создания устойчивого симметричного блочного шифрования. В мире со стороны таких ученых как B.Schneier, Y.Dodis, N.Ferguson, J.Kelsey, M.Matsui, L.Knudsen, N.Courtois, N.Harris, E.Biham, A.Shamir, J.L.Massey, Р.Олейников, О.Казимиров, Л.Бабенко, Е.Ищукова ведутся научно-исследовательские работы по разработке алгоритма шифрования и криптостойких отображений, а также по их криптоанализу.

В Узбекистане со стороны научных групп под руководством П.Ф.Хасанова, М.Арипова, С.К.Ганиева, М.М.Каримова, Д.Е.Акбарова, Б.Ф.Абдурахимова, Г.У.Джураева, Г.Н.Туйчиева, А.Б.Сатторова, Х.П.Хасанова, Д.М.Курьязова проведены исследования, связанные с разработкой методов криптографической защиты информации и вопросами оценки криптографических алгоритмов.

Вместе с тем, недостаточно внимания уделялось совершенствованию адгоритма симметричного шифрования O'z DSt 1105:2009 и его оценке с применением интегральных и алгебраических методов критоанализа.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научного проекта согласно плану научно-исследовательских работ Ташкентского университета информационных технологий №Ф706-17 - «Исследование применения биометрико – криптографических технологий в информационных системах» (2017-2018).

Целью исследования является совершенствование алгоритма симметричного шифрования O'z DSt 1105:2009 и оценка его устойчивости с применением интегральных и алгебраических методов криптоанализа.

Задачи исследования:

анализ симметричных блочных алгоритмов шифрования и методов оценки их устойчивости;

оценить устойчивость алгоритма симметричного шифрования O'z DSt 1105:2009 с помощью интегрального и алгебраического методов криптоанализа;

разработать алгоритм шифрования O‘z DSt 1105:2009 и его программное обеспечение, усовершенствованного с точки зрения оперативности и безопасности;

оценить устойчивость усовершенствованного алгоритма шифрования O‘z DSt 1105:2009.

Объект исследования является алгоритмы симметричного шифрования и процессы криптоанализа.

Предмет исследования является совершенствование алгоритма симметричного шифрования O‘z DSt 1105:2009, а также методов оценки его устойчивости с помощью интегральных и алгебраических криптоанализов.

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

Научная новизна исследования заключается в следующем:

устойчивость алгоритма симметричного шифрования O‘z DSt 1105:2009 оценена с использованием методов интегрального и алгебраического криптоанализа;

разработан алгоритм шифрования O‘z DSt 1105:2009, улучшенный статическим подбором параметров для методов подстановки и смешивания отражений;

разработан алгоритм генерации раундовых ключей на основе отображений, использованных в совершенствованном алгоритме симметричного шифрования O‘z DSt 1105:2009;

устойчивость алгоритма симметричного шифрования O‘z DSt 1105:2009 оценена с использованием методов интегрального и алгебраического криптоанализа.

Практические результаты исследования заключаются в следующем:

разработаны программные средства, позволяющие оценивать алгоритм шифрования O‘z DSt 1105:2009 с использованием методов алгебраического и интегрального криптоанализа;

разработан программное средство алгоритма симметричного шифрования O‘z DSt 1105:2009, усовершенствованного для обеспечения конфиденциальности информации;

разработан алгоритм и программное средство генерации раундовых ключей на основе ключей шифрования разной длины.

Достоверность результатов исследования. Достоверность результатов исследования обосновывается реальным и экспериментальным анализом, потвержденным с помощью методов категоричного сравнения и результатами ряда других исследований, а также полученным из методов криптоанализа криптографических алгоритмов.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования объясняется оценкой симметричных блочных шифров с использованием методов интегрального и

алгебраического криптоанализа, а также возможностью применения предложенного алгоритма генерации раундовых ключей в современных симметричных блочных шифрах.

Практическая значимоть результатов исследования обусловлено возможностью использования в шифровании данных предложенного генератора раундового ключа и усовершенствованного алгоритма симметричного шифрования O'z DSt 1105:2009.

Внедрение результатов исследования. На основании полученных результатов по предложенному генератору раундового ключа и усовершенствованному алгоритму шифрования O'z DSt 1105:2009:

результаты программного средства и криптоанализа усовершенствованного алгоритма шифрования O'z DSt 1105:2009 внедрен в ГУП «UNICON.UZ» (Справка Министерства по развитию информационных технологий и коммуникаций № 33-8/2358 от 01 апреля 2021 г.). В результате научного исследования усовершенствованный алгоритм шифрования данных позволил обеспечить конфиденциальность данных в национальных безопасных электронных системах;

на основе статистического выбора параметров в методах перестановки и смешивания, непосредственной генерации раундовых ключей программного средства усовершентсвованного алгоритма шифрования O'z DSt 1105:2009 внедрена в унитарное предприятие многофункционального информационного центра «SSP Maroqand» города Ташкент (Справка Министерства по развитию информационных технологий и коммуникаций № 33-8/2358 от 01 апреля 2021 г.). Программное средство усовершенствованного алгоритма шифрования O'z DSt 1105:2009 позволило шифровать данные клиента со скоростью 300 Кбит/с;

программное средство усовершентсвованного алгоритма шифрования O'z DSt 1105:2009, подход для генерации S блоков и алгоритмов генерации раундовых ключей внедрен в учебном процессе для курсантов в рамках предмета «Методы криптографии» кафедры военного института Информационных технологий и связи Министерства обороны (Справка Министерства по развитию информационных технологий и коммуникаций № 33-8/2358 от 01 апреля 2021 г.). В результате научного исследования программное средство усовершентсвованного алгоритма шифрования O'z DSt 1105:2009 позволило шифровать быстрее чем действующий алгоритм на 22 КБайт/с.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 2 международных и 10 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме диссертации опубликовано в общей сложности 24 научных работ, из них 9 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 4 – в иностранных и 5 – в республиканских журналах, а также получены 3 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 115 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

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.

Первая глава диссертации, озаглавленная как **«Анализ алгоритмов симметричного блочного шифрования»**, посвящена роли алгоритмов симметричного блочного шифрования в криптографии, областям применения и методам их создания. Также описаны методы криптоанализа алгоритмов симметричного блочного шифрования и результаты криптоанализа современных алгоритмов симметричного блочного шифрования.

Криптографическая защита занимается предотвращением использования информации киберпреступниками или пользователями, отличными от законного получателя, обеспечивая возможность защиты конфиденциальности, целостности и отказа информации, хранящейся, обрабатываемой и передаваемой по сети.

Поскольку алгоритмы симметричного блочного шифрования являются быстрыми и очень устойчивыми, они широко используются на практике, и в большинстве стран есть свои собственные стандартные алгоритмы в этой области. Существует 5 типов симметричных блочных кодов в соответствии с их внутренней структурой: сети перестановки-замены (Substitution Permutation Networks, SPN), сеть Фейстеля (Feistel networks), добавление-поворачивание-XOR Add-Rotate-XOR, ARX), на обоснованные и гибридные виды регистра сдвига с нелинейной обратной связью (non-linear feedback shift register, NLFSR). В настоящее время существует множество государственных стандартов (O'z DSt 1105:2009, ГОСТ Р 28147-89, AES) на базе SPN и сети Фейстеля.

Практическое широкое применение симметричного блочного шифрования, в свою очередь, требует их оценки с точки зрения безопасности. В качестве широко распространенного метода криптоанализа симметричных блочных шифров примером можно привести линейный криптоанализ (linear cryptanalysis), дифференциальный криптоанализ (differential cryptanalysis), линейно-дифференциальный криптоанализ (linear-differential cryptanalysis), алгебраический криптоанализ (algebraic cryptanalysis) (интегральный криптоанализ (integral cryptanalysis). Результат криптоанализа характеризуется необходимыми факторами *данных (data, D), времени (time, T)* и *памяти (memory, M)*.

На основе этих факторов были проанализированы большинство современных алгоритмов симметричного блочного шифрования. Хотя результаты анализа не показывают практической слабости алгоритма, он выявляет существенные недостатки в его структуре и отображении. Это важно для создания новых симметричных блочных шифров.

Однако проведенные исследования показали, что алгоритм симметричного блочного шифрования O'z DSt 1105:2009 не оценивался с использованием методов криптоанализа, описанных выше. Поэтому в следующей главе рассматривается вопрос оценки алгоритма шифрования O'z DSt 1105:2009 с использованием алгебраического и интегрального криптоанализа.

Во второй главе диссертации под названием **«Оценка криптостойкости алгоритма шифрования O'z DSt 1105:2009 с использованием алгебраических и интегральных методов криптоанализа»** проведена алгебраический и интегральный криптоанализ алгоритма шифрования O'z DSt 1105:2009.

Алгоритм шифрования O'z DSt 1105:2009 относится к типу симметричных блочных шифров и основан на сети SPN. В алгоритме длина блока шифрования может составлять 256 бит, а ключи шифрования могут быть 256 или 512 бит. Алгоритм в основном состоит из двух частей, процессов генерации и шифрования/расшифровки ключей. На этапе генерации ключей выполняются этапы генерации раундовых ключей и блоков S с использованием ключа шифрования и функционального ключа. Эти этапы осуществляются путем последовательного выполнения следующих функций *ShaklSeansKalitBayt()*, *ShaklSeansKalit()*, *ShaklBosqichKalit()*.

Также в структуре алгоритма используются четыре функции отражения. Это, такие отражения как *Qo'shBosqishKalit ()→X, Aralash()→A, Sur()→S* ва *BaytAlmash()→B. Aralash()* и *BaytAlmash()* отражения, используемые в алгоритме, считаются отражениями без основной линии, и считается важным в обеспечении криптостойкости алгоритма. Поэтому криптоанализ в основном проводится в отношении этих отражений. Характеристики систем уравнений, построенных по отношению к таблицам, используемым при отражении *BaytAlmash()* в проведенном алгебраическом криптоанализа, представлены в таблице 1 ниже.

Таблица - 1

Параметры систем уравнений, построенных на таблицах *BaytAlmash()*, сгенерированных из различных ключей

№	Нелинейность	Алгебраический иммунитет	Количество уравнений	№	Нелинейность	Алгебраический иммунитет	Количество уравнений
1.	92	3	441	6.	90	3	441
2.	90	3	441	7.	92	3	441
3.	90	3	441	8.	94	3	441
4.	94	3	441	9.	94	3	441
5.	94	3	441	10.	70	3	441

Результаты были получены при анализе 10 диаматриц специальной структуры размером 4×4. В этом случае наименьшая степень порождаемых систем алгебраических уравнений равна Deg=7. Максимальное количество сгенерированных одночленов составляет 17742 единиц (таблица 2).

Таблица – 2

Параметры систем уравнений, представляющих диагональные элементы для диаматриц, сформированных из различных ключей

№	Степень уравнений (единицы)								Количество одночленов
	Deg=1	Deg=2	Deg=3	Deg=4	Deg=5	Deg=6	Deg=7	Deg=8	
1.	4	4	4	4	4	4	4	4	14993
2.	4	6	2	6	2	4	4	4	13395
3.	4	4	4	4	4	4	4	4	14993
4.	4	6	2	5	3	4	4	4	17674
5.	4	4	4	4	4	4	4	4	4784
6.	4	8	0	7	1	7	1	4	7036
7.	4	4	4	4	4	4	4	4	14993
8.	4	7	1	7	2	6	1	4	17742
9.	4	4	9	3	3	3	3	3	3674
10.	4	5	3	4	4	4	4	4	15240

Кроме того, было установлено, что замена четырех отражений, используемых в алгоритме шифрования O'z DSt 1105:2009, влияет на общую криптографическую оценку алгоритма. Общее количество перестановок четырех функций отражения составило 24 единицы, для каждого из случаев был проведен алгебраический криптоанализ, и были получены следующие результаты (таблица 3).

Таблица - 3

Индикаторы уравнений, построенных для случаев замены места отражений алгоритма шифрования O'z DSt 1105:2009.

	Порядок отражений	1-й раунд			I	II	2-й раунд		I		II
		TS	Deg	NS			TS	Deg	NS		
1	2	3	4	5	6	7	8	9	10	11	12
1.	XASB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
2.	XABS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
3.	XBSA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
4.	XBAS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
5.	XSBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
6.	XSAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
7.	AXSB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
8.	AXBS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
9.	ABSX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
10.	ABXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
11.	ASBX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
12.	ASXB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
13.	SAXB	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
14.	SABX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
15.	SBXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
16.	SBAX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
17.	SXBA	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
18.	SXAB	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
19.	BASX	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}
20.	BAXS	256	1	2^8	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}

1	2	3	4	5	6	7	8	9	10	11	12
21.	BXSA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
22.	BXAS	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
23.	BSXA	441	3	2^{10}	2^{30}	1	256	8	2^{15}	2^{45}	2^{73}
24.	BSAX	256	1	2^{8}	-	2^{14}	256	8	2^{15}	2^{45}	2^{73}

Примечание: TS - количество уравнений, Deg - уровень, NS - количество неизвестных, I - сложность решения ТС ($\approx O(NS)^3$), II - объем памяти, необходимый для хранения ТС (байт)

Из результатов данного анализа можно сделать вывод, что для хранения системы уравнений, сформированной после второго раунда, при оценке алгоритма шифрования O'z DSt 1105:2009 с использованием алгебраического метода криптоанализа требуется 273 байта памяти. Отсутствие возможности обеспечения этого требуемого объема памяти указывает на то, что алгоритм справляется с алгебраическим методом криптоанализа после второго раунда.

Кроме того, алгоритм шифрования O'z DSt 1105:2009 был оценен с использованием метода интегрального крипто анализа. Результат исследования показал, что отражение *Aralash()*, используемое в алгоритме, обеспечивает его устойчивость к интегральному криптоанализу. Ниже приведены результаты поиска ключа к последнему раунду поддержки интегрированного метода интегрального криптоанализа по алгоритму O'z DSt 1105:2009 с четырьмя раундами, показанные на рис.1.

Здесь: А - активный (A_l- если составные части расположены в различном порядке) или П - пассивный или Д - смешанный ($Д_0$- если сбалансированный, $Д_1$- если несбалансированный).

Результат анализа показал неопределенность значений K_1^4, K_5^4, K_{14}^4, K_{15}^4, K_{20}^4, K_{21}^4, K_{27}^4, K_{30}^4, K_{31}^4 одного и того же раундового ключа в соответствии характеристикам отражения *BaytAlmash()* в конце 2-го раунда. Поиск этих ключевых байтов с использованием метода полного выбора требует вычисления 2^{72} единиц.

Третья глава диссертации под названием **«Разработка усовершенствованного алгоритма шифрования»** посвящена вопросам выбора S таблиц для *BaytAlmash()* отражения алгоритма шифрования O'z DSt 1105:2009, выбора диаматриц, статическим образом для *Aralash()* отражения. Кроме того, был разработан алгоритм независимой генерации раундовых ключей и на их основе усовершенствован алгоритм шифрования DSt 1105: 2009.

В алгоритме шифрования O'z DSt 1105:2009 для *BaytAlmash* () отражения S таблицы, для *Aralash()* отражения диаматрицы динамически генерируют ключей шифрования и функционала. Статический выбор этих динамических переменных позволяет провести относительно точную криптографическую оценку алгоритма. Кроме того, генерация динамических переменных перед каждым шифрованием в алгоритме снижает его скорость.

Для алгоритма шифрования O'z DSt 1105:2009, необходимо проверить, что S соответствует его криптографическим требованиям при генерации статических таблиц. Поэтому вместо двух таблиц S в отражении *BaytAlmash()*

поставлены требования использовать следующие параметризованные таблицы:

1. Таблица размером 8×8 (S_1) с максимальным индикатором $N(S)$ и минимальным показателем δ;
2. Таблица размером 8×8 (S_1) с максимальным индикатором $Al(S)$.

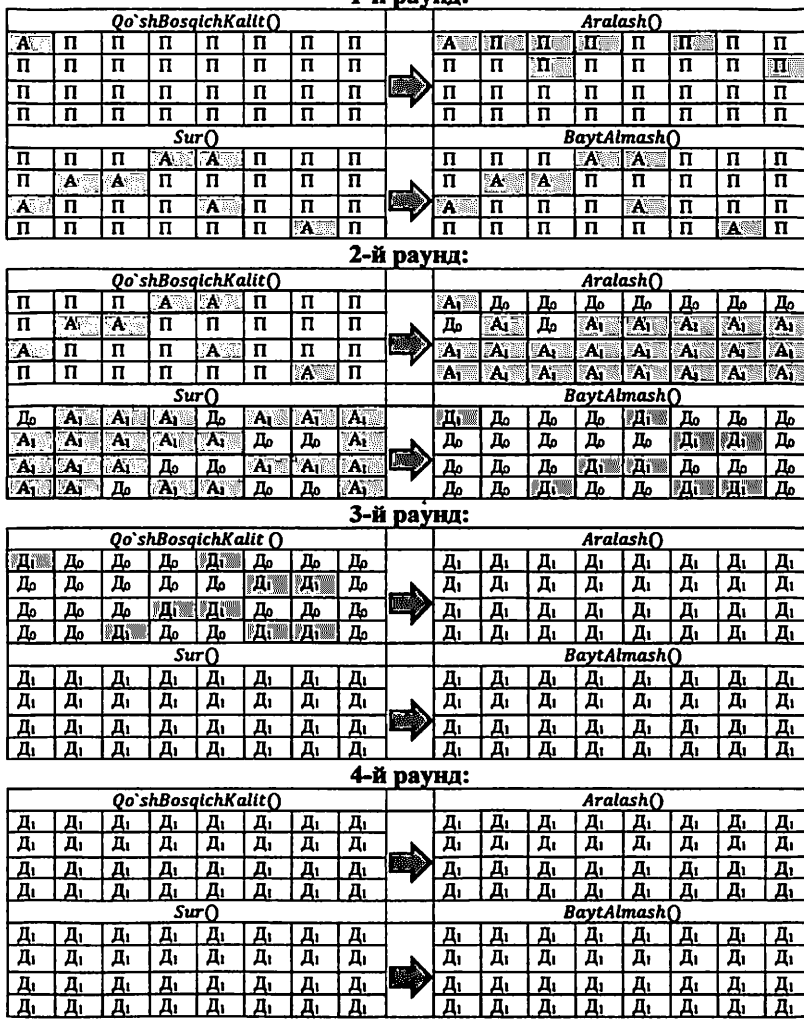


Рисунок 1. Интегральный криптоанализ алгоритма шифрования O'z DSt 1105:2009

При создании S таблицы удовлетворяющий первое требование был использован подход, используемый в AES стандарте

$$y = (Ax^{-1} \oplus c) mod\ m(x)$$

Где: y - исходящий байт, A – аффинная матрица, x^{-1}- инверсия входящего байта, $c = 0x63$ - константа.

При оценке криптографических требований таблицы S_1, сформированной на основе приведенных выше правил, были получены следующие результаты (Таблица 4).

Таблица - 4

Результаты оценки сгенерированных S_1 и S_2 таблиц

Факторы оценки		Значение (S_1)	Значение (S_2)
Баланс		True	True
Регулярность		True	True
Нелинейность, $N(S)$		112	104
Корреляционный иммунитет, (CI)		0	0
Минимальная степень, deg		7	7
Максимальное значение в таблице матрицы разделения, δ		4	8
$D(S)$		133120	194944
Стабильная эффективность лавина, SAC		False	False
Алгебраический иммунитет	AI (S)	2	3
	TS(S)	39	441

Примечательным аспектом этих результатов является то, что нелинейная скорость сгенерированной таблицы S_1 является максимальным $N(S)$, а показатель δ-минимальным, что гарантирует устойчивость алгоритма линейному, дифференциальному и линейно-дифференциальному криптоанализу. С другой стороны, алгоритм также должен быть устойчивым к алгебраическому анализу (эти два требования не могут быть выполнены одновременно). Поэтому, при генерации второй таблицы – S_2 в алгоритме стоит обратить внимание на то, что она обладает ее высоким алгебраическим иммунитетом.

Поэтому было определено следуюущие утверждения для создаваемой таблицы S_2:

1-утверждение. $AI(S) = 3$, $N_{TS} = 441$ и $N(S) \geq 104$ свойственны для таблицы оптимальной S(8×8) и с максимальным значением параметра *AI*.

При создании таблиц S, соответствующих приведенному выше утверждению, были предприняты следующие два шага:

1. Получение таблицы S(8×8), где степень нелинейности выше (N(S)=112.
2. Взаимная перестановка случайного N-го элемента таблицы S (8×8).

Эксперименты проводились для случая, когда значение N было равно 22, и была сгенерирована S_2 с криптографическими характеристиками, приведенными в таблице 4 .

Алгебраический иммунитет таблицы S_2 высока, а ее использование в структуре алгоритма гарантирует ее устойчивость к алгебраическому криптоанализу.

Следующим элементом, который динамически генерируется из функционального ключа в структуре алгоритма шифрования O'z DSt 1105:2009, являются специально структурированные диаматрицы. Для статического использования этих специально структурированных диаматриц в структуре алгоритма была выполнена следующая последовательность операций:

1. Генерация диаматриц K_1 и K_2 на основе случайно выбранных ключей.

2. Определить, на сколько битов влияет изменение одного бита на пару диматриц K_1 и K_2 в каждом раунде.

В эксперименте было сгенерировано 200 различных пар диаматриц K_1 и K_2. Были определены параметры распределения после каждого раунда пар диаматриц (*SAC* - строгая эффективность Лавина). Полученные результаты показали, что алгоритм шифрования O'z DSt 1105:2009 достигнет максимального уровня распределения после 3-го раунда для всех сгенерированных пар диаматриц. С другой стороны, также было показано, что одну из сгенерированных диматрических пар K_1 и K_2 можно использовать статически. Следующие две пары диаматриц были выбраны среди сгенерированных пар диаматриц для статического использования.

$$K_1 = \begin{vmatrix} 149 & 157 & 87 & 182 \\ 92 & 149 & 92 & 92 \\ 13 & 77 & 149 & 13 \\ 157 & 68 & 184 & 149 \end{vmatrix} \qquad K_2 = \begin{vmatrix} 157 & 150 & 197 & 66 \\ 52 & 157 & 52 & 52 \\ 86 & 233 & 157 & 86 \\ 184 & 241 & 69 & 157 \end{vmatrix}$$

Для процесса шифрования и дешифрования определяются и используется диаматрицы, обратные этим двум диаматрицам.

Обычно разработка раундовых ключей основана на использовании ключа предыдущего раунда. Например, в алгоритмах шифрования AES и O'z DSt 1105:2009. В соответствии с этим ключ первого раунда используется для генерации ключа следующего раунда, и т.д. Это, в свою очередь, требует большого объема памяти для хранения раундовых ключей. В частности, в процессе дешифрования, основанном на обратном использовании раундовых ключей, требует, чтобы ключи были сначала сгенерированы и сохранены. Поэтому требуется формирование функции $\phi()$ – которая предотвращает существующие проблемы и способна самостоятельно обобщать ключи каждого раунда:

$$K_i = \phi(K, i).$$

Где, K – ключ шифрования, i – количество раундов и K_i - i – ключ раунда. Другими словами, каждый раундовый ключ генерируется на основе ключа шифрования и количества раундов. Кроме того, разрабатываемый генератор ключа раунда должен отвечать следующим требованиям:

- невозможность вычислить ключ шифрования из раундового ключа (односторонность);

- получать ключи шифрования разной длины и генерировать на выходе раундовые ключи нужной длины.

На основе вышеизложенных требований и рекомендаций был разработан алгоритм генерации раундового ключа для усовершенствованного алгоритма шифрования O'z DSt 1105:2009 (рис. 2).

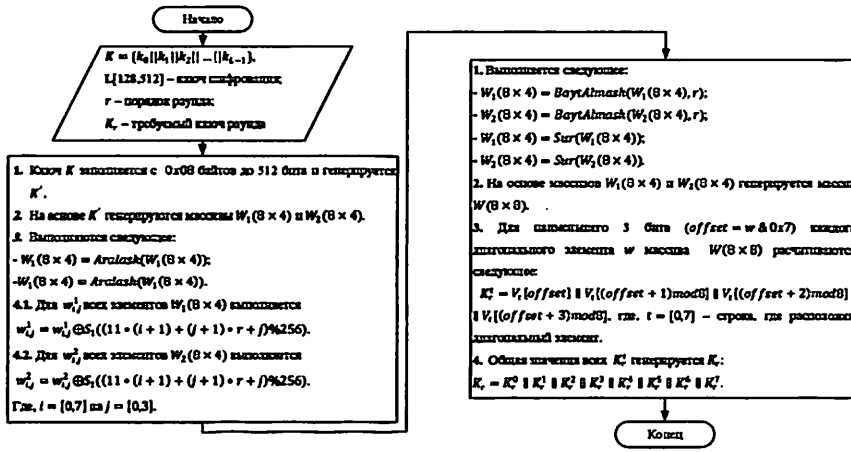


Рисунок 2. Блок-схема алгоритма генерации раундового ключа (для 256-битного раундового ключа)

Оценка псевдослучайных последовательностей, генерируемых разработанным генератором ключей, проводилась с использованием набора статистических тестов NIST. При тестировании случайным образом выбирался исходный входной ключ шифрования, длина которого составляла 128, 192, 256, 512 бит, а длина-128 бит для входного случая слабых ключей (состоящих из 00, FF, 01, E1 и EF байтов). Результаты тестирования представлены в таблице 6.

Таблица - 6

Результаты статистического тестирования псевдослучайных последовательностей

№	Начальная длина ключа и уровень случайности	Образцы				
		1	2	3	4	5
1.	128 бит и случайный	15/16	15/16	15/16	15/16	14/16
2.	192 бит и случайный	15/16	15 /16	15 /16	15/16	15/16
3.	256 бит и случайный	15/16	15/16	15/16	15/16	15/16
4.	512 бит и случайный	15/16	15/16	14/16	14/16	15/16
5.	128 бит и слабые места (0x00, 0xFF, 0x01, 0xE1 и 0xEF)	15/16	13/16	13/16	15/16	15/16

Полученные результаты тестирования показали, что разработанный генератор ключей генерирует раундовые ключи, устойчивые к ключам шифрования разной длины и уровня случайности.

Последовательность шифрования и дешифрования алгоритма шифрования O‘z DSt 1105:2009, усовершенствованного на основе вышеупомянутых отражений и функций раунда, показана на рисунке 3.

Четвертая глава диссертации под названием **«Оценка усовершенствованного алгоритма шифрования O‘z DSt 1105:2009»** посвящена оценке усовершенствованного алгоритма шифрования O‘z DSt 1105:2009 на основе характеристик скорости и надежности.

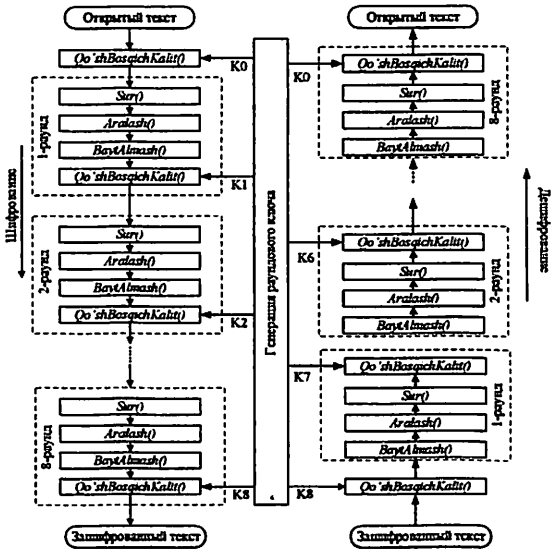


Рисунок 3. Последовательность шифрования и дешифрования усовершенствованного алгоритма шифрования O‘z DSt 1105:2009

Функции отражения, доступные в усовершенствованном алгоритме шифрования O‘z DSt 1105:2009, остались не измененными. Выше упоминалось, что изменение порядка функций отражения влияет на устойчивость алгоритма шифрования. Результаты интегрального анализа для 6 случаев, в которых выполнялась строгая эффективность Лавина из всех вариантов четырех функций отражения, приведены в Таблице 7 ниже.

Таблица - 7

Влияние выходных байтов после 2-го раунда для различного порядка функций отражения

№	Режим отражения	Влияние	№	Режим отражения	Влияние
1.	Б → Q → S → A	12	4.	S → Q → A → B	15
2.	Q → S → B → A	15	5.	S → A → B → Q	12
3.	Q → S → A → B	12	6.	S → A → Q → B	15

Эти результаты были рассчитаны для 4-раундового варианта усовершенствованного алгоритма шифрования O‘z DSt 1105:2009, в котором количество открытых текстов составило 2^8.

Например, для последовательного варианта отражения S → A → B → Q усовершенствованного алгоритма шифрования O'z DSt 1105:2009, неизвестность элементов 12 байтов после 2-го раунда обосновывается следующим образом.

Выбирается множество, в котором байтовый элемент массива состояний становится активным, и наблюдается его балансирующие свойства выходных значений S→A→B→Q из каждого раунда. При наличии набора шифровальных текстов T_i, соответствующих выбранным открытым текстам, последовательность процесса расшифровки выглядит следующим образом:

$$C_i = Sur(Aralash(BaytAlmash(Qo'shBosqichKalit(T_i, K^4))))$$

Где, C_i массив представляет состояние на входе четвертого раунда. На всех (от 0 до 255) значениях ключа K^4, которые могут принимать байты K_q^4 $(1 \le q \le 32)$, C_i передаётся через отражения массива третьего райнда:

$$R_{iq} = Sur\left(Aralash\left(BaytAlmash(C_i)\right)\right)$$

После этого рассчитывается сумма XOR значений R_{iq}:

$$XOR = R_{1q} \oplus R_{2q} \oplus R_{3q} \oplus R_{mq}$$

Если $XOR = 0$, то раундовый ключ K_q^4 $(1 \le q \le 32)$ добавляется в список ключей-кандидатов.

Основываясь на результатах приведенного выше анализа, можно сказать, что использование метода интегрального криптоанализа к усовершенствованному алгоритму шифрования на основе 4-раундового алгоритма шифрования O'z DSt 1105:2009 с отражением порядка S→A→B→Q на основе выбранных открытых текстов 2^8 можно найти K_2^4, K_4^4, K_5^4, K_7^4, K_9^4, K_{10}^4, K_{11}^4, K_{12}^4, K_{14}^4, K_{17}^4, K_{19}^4, K_{20}^4, K_{21}^4, K_{22}^4, K_{25}^4, K_{28}^4, K_{29}^4, K_{30}^4, K_{31}^4, K_{32}^4 байта (всего 160 бит) ключа на выходе этого раунда в соответствии со свойствами отражения *BaytAlmash()* в конце 2-го раунда. Согласно свойствам отражения *BaytAlmash()* в конце 2-го раунда общее количество вариантов в методе полного выбора остальных байтов K_1^4, K_3^4, K_6^4, K_8^4, K_{13}^4, K_{15}^4, K_{16}^4, K_{18}^4, K_{23}^4, K_{23}^4, K_{24}^4, K_{26}^4, K_{27}^4 ключа 4-го раунда равно 2^{96}.

Кроме того, для криптографической оценки усовершенствованного алгоритма шифрования O'z DSt 1105:2009 использовался метод алгебраического криптоанализа. Эксперименты показали, что в *Aralash()* и *BaytAlmash()* отражения в алгоритме шифрования O'z DSt 1105:2009 являются основными отражениями, влияющими на уровень системы уравнений, представляющей алгоритм и количество неизвестных.

Алгебраический криптоанализ, примененный для отражения *BaytAlmash()* проведен для S_1 ва S_2 таблиц, используемых в усовершенствованном алгоритме шифрования O'z DSt 1105:2009. Согласно ему, количество уравнений 2-го и 3-го уровня для таблицы S_1 составляет 39 и 471 соответственно, а количество уравнений 3-го уровня для таблицы S_2 составляет 441.

Также был проведен алгебраический криптоанализ для диагональных элементов диаматриц, используемых в *Aralash()* отражении усовершенствованного алгоритма шифрования.

Согласно полученному результату, общее количество одночленов в уравнениях зависимости входных и выходных битов от диаматрицам со специальной структурой K_1, K_{2t}, используемых при шифровании, составило 14 993.

В заключение, основываясь на результатах проведенных экспериментов, можно увидеть, что независимая генерация раундовых ключей удвоит устойчивость алгоритма к алгебраическому криптоанализу после 2-х раундов.

Кроме того, усовершенствованный алгоритм шифрования O'z DSt 1105:2009 также был оценен с точки зрения скорости. При этом, были разработаны программные средства существующих и усовершенствованных алгоритмов шифрования O'z DSt 1105:2009. Также, использовалась ГОСТ Р 28147-89 и библиотека языка программирования C# алгоритма шифрования AES. Для получения скорости шифрования с высоким разрешением использовалось программное обеспечение ANTS Performance Profiler для программного обеспечения среды .NET (рисунок 4).

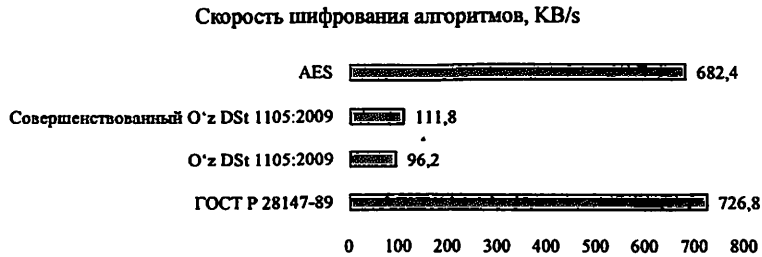


Рисунок 4. Скорость шифрования данных алгоритмов

Причиной обработки данных с низкой скоростью со стороны существующих и усовершенствованных алгоритмов шифрования O'z DSt 1105:2009 является использование операции умножения специально структурированных диаматриц при *Aralash()* отражении. Тем не менее, усовершенствованный алгоритм шифрования O'z DSt 1105:2009 отметил более высокую скорость 22 Кбайт/с по отношению к существующему алгоритму шифрования.

ЗАКЛЮЧЕНИЕ

В результате исследовательской работы над диссертацией «Совершенствование алгоритма симметричного шифрования и оценка с использованием методов криптоанализа» были сделаны следующие выводы:

1. Проанализированы алгоритмы симметричного блочного шифрования и методы оценки их устойчивости. В результате анализа было выявлено, широкое распространение методов линейного, дифференциального,

интегрального и алгебраического криптоанализа при оценке устойчивости современных симметричных блочных шифров.

2. Алгоритм шифрования O'z DSt 1105:2009 проанализированы по составным частям и структурам. В результате анализа было обнаружено, что в отражениях *BaytAlmash()* и *Aralash()* алгоритма шифрования O'z DSt 1105: 2009 сгенированные динамическим образом таблицы и диаматрицы на основе сеансового ключа не позволяет точно оценить алгоритм.

3. Устойчивость алгоритма шифрования O'z DSt 1105:2009 оценивалась с использованием методов алгебраического криптоанализа. Поскольку результат криптоанализа показывает, что для поиска ключа для раунда 2 требуется 2^{73} байт памяти, МША устойчив к алгебраическому криптоанализу.

4. Устойчивость алгоритма шифрования O'z DSt 1105:2009 оценивалась с использованием методов интегрального криптоанализа. Результат криптоанализа показал, необходимось выполнение 2^{72} операций для нахождения ключа шифрования после отражения *BaytAlmash()* во 2-раунде.

5. В алгоритме шифрования O'z DSt 1105:2009, было усовершенствовано отражение *BaytAlmash()* на основе статических таблиц S_1 с высокой нелинейностью и S_2 высокой алгебраическим иммунитетом, отражение *Aralash()* на основе статических специально структурированных диаматриц 4×4 обспечивающий лавинный эффект. В результате стало возможным точно оценить алгоритм.

6. Разработан независимый алгоритм генерации раундовых ключей. Разработанный алгоритм зафиксировал 92% уровень случайности при оценке на основе набора статистических тестов NIST.

7. Усовершенствованный алгоритм шифрования O'z DSt 1105:2009 был оценен с помощью алгебраического метода криптоанализа. В результате анализа было установлено, что независимая генерация раундовых ключей удвоила устойчивость алгоритма к алгебраическому криптоанализу после 2-го раунда.

8. Усовершенствованный алгоритм шифрования O'z DSt 1105:2009 оценен с помощью интегрального метода криптоанализа. В результате анализа было обнаружено, что использование отражений раундовой функции в различных процедурах влияет на устойчивость алгоритма к интегральному криптоанализу.

9. Разработано программное средство усовершенствованного алгоритма шифрования O'z DSt 1105:2009. В результате анализа было установлено, что статическое использование специально структурированных диаматриц и S таблиц увеличивает скорость работы алгоритма.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES
DSc.13/30.12.2019.T.07.01 AT TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

ALLANOV ORIF MENGLIMURATOVICH

IMPROVEMENT OF SYMMETRIC BLOCK ENCRYPTION ALGORITHM AND EVALUATION USING CRYPTANALYSIS METHODS

05.01.05 – Methods and systems of information protection. Information Security

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent-2021

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2021.2.PhD/T1940.

The dissertation has been prepared at Tashkent University of Information Techologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website www.tuit.uz and on the website of «ZiyoNet» Information and educational portal www.ziyonet.uz.

Scientific adviser:	**Abdurakhimov Bakhtiyor Fayzievich** Doctor of Physical-Mathematical Sciences, Professor
Official opponents	**Juraev Gayrat Umarovich** Doctor of Physical-Mathematical Sciences, Docent
	Yusupov Bakhodir Karamatovich Doctor of Philosophy on technical sciences
Leading organization:	**Scientific-Engineering and Marketing researches Center "UNICON.UZ"**

The defense will take place «____» _____ 2021 at _____ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No.___). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «____» _____ 2021 y.
(mailing report No. ___ on «____» _____ 2021 y.).

R.Kh. Khamdamov
Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

F.M. Nuraliev
Scientific secretary of scientific council awarding scientific degrees, Doctor of Technical Sciences, Docent

S.K.Ganiev
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Technical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to improve the encryption algorithm O'z DSt 1105:2009 and assess its reliability using integral and algebraic cryptanalysis methods.

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

The scientific novelty of the research work is as follows:

the encryption algorithm O'z DSt 1105: 2009 was evaluated using the methods of integral and algebraic cryptanalysis;

O'z DSt 1105: 2009 encryption algorithm that improved by static selection of parameters for methods of substitution and mixing of reflections was developed;

an algorithm for generating round keys based on the reflections used in the improved symmetric encryption algorithm O'z DSt 1105: 2009 has been developed;

the improved encryption algorithm O'z DSt 1105: 2009 has been evaluated using the methods of integrated and algebraic cryptanalysis.

Implementation of the research results. Based on the results obtained for the proposed round key generator and the improved encryption algorithm O'z DSt 1105: 2009:

the results of the software and cryptanalysis of the improved encryption algorithm O'z DSt 1105: 2009 was implemented in the State Unitary Enterprise (SUE) "UNICON.UZ" - Center for scientific, technical and marketing research (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan No. 33-8/2358 on 01 april 2021 y.) As a result of scientific research, an improved data encryption algorithm made it possible to ensure the confidentiality of data in national secure electronic systems;

on the basis of the statistical selection of parameters in the methods of permutation and mixing, direct generation of round keys of the software for the improved encryption algorithm O'z DSt 1105: 2009 was introduced into the unitary enterprise of the multifunctional information center "SSP Maroqand" in Tashkent (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan No. 33-8/2358 on 01 april 2021 y.). The O'z DSt 1105: 2009 Advanced Encryption Algorithm software enabled encryption of client data at a rate of 300 Kbps;

software for the improved encryption algorithm O'z DSt 1105: 2009, the approach for generating S blocks and algorithms for generating round keys has been implemented in the educational process for cadets within the framework of the subject "Cryptography Methods" of the Department of the Military Institute of Information Technology and Communications of the Ministry of Defense (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan No. 33-8/2358 on 01 april 2021 y.). As a result of scientific research, the advanced encryption algorithm software O'z DSt 1105: 2009 made it possible to encrypt faster than the current algorithm by 22 KB/s.

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 115 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (Часть I; Part I)

1. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M., Algebraic Cryptanalysis of O'z DSt 1105:2009 Encryption Algorithm // Information Sience and Communication Technologies (ICISCT), International conference on. – IEEE, Toshkent 2020. –P. 1-6. (05.00.00; 30.10.2020 №368–сон раёсат қарори). (Csopus, **DOI:** 10.1109/ICISCT50599.2020.9351469).
2. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O., Boykuziyev I.M., Differential Collisions in SHA-1 // Information Sience and Communication Technologies (ICISCT), International conference on. –IEEE, Toshkent 2020. –P. 1-5. (05.00.00; 30.10.2020 №368–сон раёсат қарори). (Scopus, **DOI:** 10.1109/ICISCT50599.2020.9351441).
3. Khudoykulov Z.T., Islomov Sh.Z., Allanov O.M., Mardiyev U.R., A Practical implementation of fingerprint based fuzzy commitment scheme// European Science Review, -Austria, Vienna, 2018, -№ (5-6) -P. 108-112 (05.00.00; №3). (IF=1.41).
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. Volume 29, No. 5, 2020, -P. 12397-12412 (05.00.00; №17). (IF=0.41).
5. Абдурахимов Б.Ф., Примкулов Б.Ш., Худойқулов З.Т., Алланов О.М., Симметрик блокли шифрлаш усулларининг таҳлили // ТошДТУ хабарлари. –Тошкент, 2017, №2 – Б. 30-35, (05.00.00; №16)
6. Иргашева Д.Я., Худойқулов З. Т., Исломов Ш.З., Алланов О., Бармоқ изига асосланган аутентификациялаш усулларини таҳлили// Ахборотқоммуникациялар: Тармоқлар, Технологиялар, Ечимлар. Ҳар чорак илмий-техник журнал, 2018, № 4(48) –Б. 45-54 (05.00.00; №2).
7. Худойқулов З.Т., Алланов О., Холимтаева И.У., Замонавий хэш функсияларинг хавфсизлик ва тезлик хусусиятлари асосидаги таҳлили // Ахборотқоммуникациялар: Тармоқлар, Технологиялар, Ечимлар. Ҳар чорак илмий-техник журнал, 2018, № 2(46) –Б. 45-53 (05.00.00; №2).
8. Алланов О. AES конкурси финалчиларига қаратилган криптотаҳлиллар натижалари // Муҳаммад ал-Хоразмий авлодлари, Илмий-амалий ва ахборот-таҳлилий журнал, 2019, 4(10) –Б. 7-10 (05.00.00; №10).
9. Абдурахимов Б.Ф., Алланов О., Худойқулов З.Т., Исломов Ш.З., DES Алгоритмининг чизиқли криптотаҳлили // Ахборотқоммуникациялар: Тармоқлар, Технологиялар, Ечимлар. Ҳар чорак илмий-техник журнал, 2019, № 3(51) –Б. 56-61 (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 //Information Sience and Communication Technologies (ICISCT), International conference on. –IEEE, Toshkent 2019. –P. 1-3. (Scopus, **DOI:** 10.1109/ICISCT47635.2019.9011917).

2. Абдурахимов Б.Ф., Алланов О., Хамидов Ш.Ж., Исследование стандарта шифрования республики узбекистан //Abstracts of III International Scientific and Practical Conferenc. London, United Kingdom -2020. –P. 196-176.

3. Абдурахимов Б.Ф., Алланов О., Шоназаров С.К., Теоретический анализ устойчивости современных алгоритмов блочного шифрования// «Высшая школа» Научно-практический журнал. №8, Уфа - 2018 г., -С. 69-72.

4. Абдурахимов Б.Ф., Алланов О., Йўлдошов М. Х., Замонавий блокли шифрлаш алгоритмларининг тезликларининг таҳлили// International conference on importance of information-communication technologies in innovative development of sectors of economy. Tashkent -2018. -Б. 421-424.

5. Худойқулов З., Алланов О. Ахборот хавфсизлигини таъминлашда ассиметрик шифрлаш усулларининг ўрни// Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». Сборник тезисов и докладов. Ташкент – 2016 г. - Б. 26-28.

6. Allanov O. Unionpay xalqaro to'lov kartalarining afzalliklari// Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». Сборник тезисов и докладов. Ташкент – 2016 г. - Б. 81-82.

7. Алланов О. Тармоқ хавфсизлигини таъминлаш усули// «Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот–коммуникация технологияларининг аҳамияти» Республика илмий-техник анжуманининг маърузалар тўплами. 3-қисм. Тошкент-2017 й. –Б. 116-118.

8. Алланов О. Криптографик хэш функцияларнинг ахборот хавфсизлигини таъминлашдаги ўрни// «Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот–коммуникация технологияларининг аҳамияти» Республика илмий-техник анжуманининг маърузалар тўплами. 3-қисм. Тошкент-2017 й. –Б. 116-118.

9. Allanov O., Asrorov A., Sodiqova D. Axborot konfidensialligini himoyalash usullari// «Таълим, фан ва ишлаб чиқариш интеграциясида инновацион технологияларни қўллаш -мамлакат тараққиётинингмуҳим омили» мавзусидаги XV республика илмий-амалий конференцияси материаллари, II қисм. Самарқанд-2018. –Б. 241-243.

10. Абдурахимов Б.Ф., Алланов О., Каримов А.А. Криптотаҳлил усулларининг истиқболлари// «Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик

муаммолари» Республика миқёсидаги илмий-техник конференция. Тошкент-2018 й., -Б. 13-16.

11. Abduraximov B., Allanov O., Djurabayev A., Kriptografik tizimlar tahlili// «Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари» Республика миқёсидаги илмий-техник конференция. Тошкент-2019 й., -Б. 68-71.

12. Abduraximov B., Allanov O., Djurabayev A., Kalit va ma'lumotlarning inkapsulyatsiyasi mexanizmlariga asoslangan kombinatorli shifrlash algoritmlari// Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари Республика миқёсидаги илмий-техник конференция. Тошкент-2019 й. -Б. 76-78.

13. Алланов О., Бойқўзиев И.М., Абдурахимов Б.Ф., Худойқулов З. Т., Модификацияланган ЎзДСт 1105:2009 шифрлаш алгоритми// Дастурга гувоҳнома №DGU 09060, Ташкент, 25.09.2020.

14. Абдурахимов Б.Ф., Алланов О., Бойқўзиев И.М., Худойқулов З. Т., Каримов А.А., Олимов И.С., Хамидов Ш.Ж., Бозоров А.Х., Курбонова Ф.Ч., ЎзДСт 1105:2009 шифрлаш алгоритмини алгебраик криптотаҳлиллаш учун ишлаб чиқилган дастурий таъминоти // Дастурга гувоҳнома №DGU 07494, Ташкент, 08.01.2020.

15. Абдурахимов Б.Ф., Алланов О., Бойқўзиев И.М., Исломов Ш.З., Мардиев У.Р., Давронова Л.У., Турсунов О.О., Тожиакбарова У.У., Ахмедова Н.Ф.,Исмоилов Х.А., Миллий стандарт шифрлаш алгоритми ўқув вариантини алгебраик криптотаҳлилаш дастурий таъминоти// Дастурга гувоҳнома №DGU 07498, Ташкент, 08.01.2020.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.