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

ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ

КУРЬЯЗОВ ДАВЛАТЁР МАТЯКУБОВИЧ

БАРДОШЛИ КРИПТОГРАФИК АЛГОРИТМЛАР ЯРАТИШ УСУЛЛАРИНИ ИШЛАБ ЧИҚИШ

05.01.05–Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ФИЗИКА–МАТЕМАТИКА ФАНЛАРИ ДОКТОРИ (DSc)
ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

ТОШКЕНТ–2022

УДК 004.056.55

Физика-математика фанлари доктори (DSc)
диссертацияси автореферати мундарижаси

Оглавление автореферата дисертации доктора (DSc)
по физико-математическим наукам

Content of dissertation abstract of the doctor
of physical and mathematical sciences (DSc)

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

КУРЬЯЗОВ ДАВЛАТЁР МАТЯКУБОВИЧ

БАРДОШЛИ КРИПТОГРАФИК АЛГОРИТМЛАР ЯРАТИШ УСУЛЛАРИНИ ИШЛАБ ЧИҚИШ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги (физика-математика фанлари)

ФИЗИКА–МАТЕМАТИКА ФАНЛАРИ ДОКТОРИ (DSc) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

ТОШКЕНТ – 2022

Фан доктори (DSc) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2021.4.DSc/FM185 рақам билан рўйхатга олинган.

Докторлик диссертацияси Ўзбекистон Миллий университетида бажарилган.

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

Илмий маслаҳатчи:	**Аринов Мирсаид Мирсидикович** физика-математика фанлари доктори, профессор
Расмий оппонентлар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Жураев Гайрат Умарович физика-математика фанлари доктори, доцент
	Туйчиев Гулом Нумонович физика-математика фанлари доктори
Етакчи ташкилот:	**Ислом Каримов номидаги Тошкент давлат техника университети**

Диссертация ҳимояси Ўзбекистон Миллий университети ҳузуридаги DSc.03/30.12.2019.FM.01.02 рақамли Илмий кенгашнинг 2022 йил «11» июня соат 14⁰⁰ даги мажлисида бўлиб ўтади. (Манзил: 100174, Тошкент ш., Олмазор тумани, Университет кўчаси, 4-уй. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, 246-02-24, e-mail: rankin@nuu.uz).

Диссертация билан Ўзбекистон Миллий университетининг Ахборот-ресурс марказида танишиш мумкин (49 рақами билан рўйхатга олинган). Манзил: 100174, Тошкент ш., Олмазор тумани, Университет кўчаси, 4-уй. Тел.: (99871) 246-02-24.

Диссертация автореферати 2022 йил «30» май куни тарқатилди.
(2022 йил 2 рақамли реестр баённомаси).

Р.Д. Алиев
Илмий даражалар берувчи илмий кенгаш раиси ўринбосари, ф.-м.ф.д., профессор

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

Г.У. Жураев
Илмий даражалар берувчи илмий кенгаш ҳузуридаги Илмий семинар раиси, ф.-м.ф.д., доцент

КИРИШ (фан доктори (DSc) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳон миқёсида криптология муаммоларини ечишда аксарият ҳолларда симметрик шифрлаш алгоритмларининг сеанс калитини аниқлаш, асимметрик алгоритмларнинг очиқ калити асосида ёпиқ калитни топиш, хэш функцияларни коллизияга учратиш ва алгоритмлар қадамларидан келиб чиқиб, амалга ошириладиган крипто-ҳужумларни ишлаб чиқиш масалаларига келтирилади. Шифрлаш алгоритмлари акслантиришларининг хоссаларини ўрганиш, янги математик мураккабликлар асосида бардошли асимметрик шифрлаш ва электрон рақамли имзо алгоритмларини ишлаб чиқиш масалалари ахборот хавфсизлиги, криптография, криптотаҳлил, амалий математика ва объектга йўналтирилган дастурлаш каби соҳалар бўйича олиб борилаётган тадқиқотларнинг объекти ҳисобланади. Шу сабабли, ахборотларни криптографик ҳимоялаш усулларини яратиш, стандарт алгоритмларни доимий бардошлик талаблари бўйича таҳлил қилиш ва такомиллаштириш ахборот хавфсизлигини таъминлаш соҳасидаги муҳим вазифалардан бири бўлиб қолмоқда.

Ҳозирги кунда жаҳонда телекоммуникация тармоғи орқали узатилаётган ахборотлар хавфсизлигини таъминлаш дастурий, аппарат-дастурий қурилмалар ёрдамида амалга оширилади ва улар криптомодулларида стандарт сифатида қабул қилинган криптографик алгоритмлардан фойдаланилади. Шунинг учун стандарт симметрик шифрлаш алгоритмларини баҳолаш, эллиптик эгри чизиқ асосида бардошли янги асимметрик шифрлаш, дискрет логарифмлаш, мураккаб модул ва эллиптик эгри чизиқда дискрет логарифмлаш мураккабликларидаги бардошли янги электрон рақамли имзо алгоритмларини яратиш мақсадли илмий тадқиқотлардан ҳисобланади.

Мамлакатимизда фундаментал фанларнинг илмий ва амалий тадбиқи сифатида ахборот хавфсизлиги, криптография ва криптотаҳлил соҳалари учун бардошли криптографик алгоритмларни ишлаб чиқиш каби долзарб йўналишларига катта эътибор қаратилиб, миллий стандарт алгоритмларни такомиллаштириш ва янгиларини яратиш бўйича салмоқли натижаларга эришилди. «Алгебра ва функционал анализ, амалий математика ва математик моделлаштириш, ҳисоблаш математикаси ва дискрет математика, эҳтимоллар назарияси ва математик статистика»[1] фанларининг устувор йўналишлари бўйича халқаро стандартлар даражасидаги илмий изланишлар олиб бориш асосий вазифалар ва фаолият йўналишлари этиб белгиланган. Қарор ижросини таъминлашда янги бардошли симметрик, асимметрик шифрлаш ва электрон рақамли имзо алгоритмларини яратиш, бардошликларини

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

баҳолаш ҳамда олинган илмий натижаларни амалиётга жорий қилиш муҳим аҳамиятга эга.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947 сонли «Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида»ги Фармони, Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60 сонли «2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида»ги Фармони, Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги ПҚ-614-сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисида»ги, Ўзбекистон Республикаси Президентининг 2017 йил 17 февралдаги ПҚ-2789-сон “Фанлар академияси фаолияти, илмий-тадқиқот ишларини ташкил ташкил этиш, бошқариш ва молиялаштиришни янада такомиллаштириш чора-тадбирлари тўғрисида”ги, Ўзбекистон Республикаси Президентининг 2017 йил 20 апрелдаги ПҚ-2909-сон “Олий таълим тизимини янада ривожлантириш чора-тадбирлари тўғрисида”ги, Ўзбекистон Республикаси Президентининг 2018 йил 27 апрелдаги ПҚ-3682-сон “Инновацион ғоялар, технологиялар ва лойиҳаларни амалиётга жорий қилиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги, Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги 242-сон «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги низомни тасдиқлаш ҳақида»ги қарорлари ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий хужжатларда белгиланган вазифаларни амалга оширишга ушбу диссертация тадқиқоти муайян даражада хизмат қилади.

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

Диссертация мавзуси бўйича хорижий илмий-тадқиқотлар шарҳи [2].

Симметрик ва асимметрик алгоритмларни ишлаб чиқиш ҳамда улар бардошлигини тадқиқ этиш бўйича илмий изланишлар жаҳоннинг етакчи олий таълим муассасалари ва илмий марказлари, жумладан: National Institute of Standards and Technology - NIST, University of California, Conterpane Internet Security (АҚШ), University of Oxford (Буюкбритания), University of Haifa, Tel Aviv University,Weizmann Institute (Исроил), Concordia Institute for Information Systems Engineering, Concordia University (Канада), Dian Ji University, Jiaotong University (Хитой), Swiss Federal Institute of Technology (Швейцария), Vienna

[2] Диссертация мавзусига доир хорижий илмий тадқиқотлар таҳлили қуйидаги манбаларга асосан бажарилган: Journal of Cryptography and Communications, Journal of Cryptology, Journal of Mathematical Cryptology, Journal of Cryptographic Engineering, International journal of Applied Cryptography, Journal of Cryptologic Research, Журнал Математические вопросы криптографии.

Technical University (Австрия), Nanyang Technological University (Сингапур), Al-Balqa Applied University, Yarmouk University (Иордания), Россия ФАнинг Математика институтлари, Криптография Академияси, Москва давлат университети, Жанубий федерал университети, Москва давлат техника университети, Россия Федерацияси Федерал Хавфсизлик хизмати (ФХХ) нинг Криптография, алоқа ва информатика институти (Россия), Белоруссия давлат университети, Информатика ва радиоэлектроника университети, Ахборот ҳимояси муаммолари илмий-текшириш институти (Белоруссия), Украина ФАнинг Амалий математика ва механика институти, Киев политехника институти (Украина), Қозоғистон миллий университети, Ахборот хавфсизлиги ва криптология институти (Қозоғистон), Ўзбекистон Миллий университети, Тошкент ахборот технологиялари университети, «UNICON.UZ» (Ўзбекистон) да кенг қамровли илмий-тадқиқот ишлари олиб борилмоқда.

Турли математик мураккабликлар асосида асимметрик шифрлаш, электрон рақамли имзо алгоритмларини ишлаб чиқиш, ГОСТ Р 34.12-2015 стандарт алгоритми таҳлили ва бардошли S-блоклар ишлаб чиқишга оид жаҳонда олиб борилган тадқиқотлар натижасида қатор, жумладан, қуйидаги илмий натижалар олинган: берилган катта разряддаги сонни туб кўпайтувчиларга ажратиш муаммосига асосланган RSA (University of California, АҚШ), чекли майдонда дискрет логарифмлаш муаммосига асосланган EL-GAMAl (National Institute of Standards and Technology, АҚШ) асимметрик шифрлаш ва электрон рақамли имзо алгоритмлари яратилган; инглиз тили сўзлари билан кодлашга асосланган янги асимметрик шифрлаш алгоритми ишлаб чиқилган ва бардошлилиги баҳоланган (Al-Balqa Applied University, Yarmouk University, Иордания); факторизация ва дискрет логарифмлаш муаммосига асосланган янги электрон рақамли имзо, жамовий имзо алгоритмлари таклиф этилган ва бардошликлари баҳоланган (Санкт-Петербург давлат электротехника университети, Россия); ГОСТ Р 34.12-2015 стандарти Кузнечик алгоритми чизиқли, дифференциал криптотаҳлил усулларига 3-раунддан сўнг бардошлилиги исботланган (Жанубий федерал университет, Россия); ГОСТ Р 34.12-2015 стандарти имитомуҳофаза функцияси бардошлилиги баҳоланган (Ахборотни ҳимоялаш соҳасида техник қўмита, Криптография академияси, Россия); маълумотни эллиптик эгри чизиқ нуқтаси ва эллиптик эгри чизиқ нуқтасини маълумот кўринишига ўтказиш алгоритмлари ишлаб чиқилган (Фанлар академияси Санкт-Петербург информатика ва автоматизация институти, Россия); махсус характеристикали чекли майдонда эллиптик эгри чизиқ асосидаги асимметрик шифрлаш алгоритми ишлаб чиқилган ва бардошлилиги баҳоланган (Санкт-Петербург давлат техника университети, Россия); эллиптик эгри чизиқда дискрет логарифмлаш масаласи мураккаблигига асосланган электрон рақамли имзо стандарт алгоритмлари ва протоколлари бардошликлари баҳоланган (Киев политехника институти, Харьков радиоэлектроника университети, Украина); алгебраик чизиқсизлик даражаси ва чизиқсизлиги юқори S-блоклар генерация қилиш усуллари яратилган

(Vienna Technical University, Katholieke Universite Leuven, Бельгия); чизиқсизлиги юқори буль функциялар генерация қилиш усуллари яратилган (Indian Statistical Institute, Ҳиндистон, University of Science and Technology of China, Хитой, University of Alabama, АҚШ).

Дунёда симметрик ва асимметрик алгоритмларнинг бир қатор устувор йўналишларида илмий тадқиқот ишлари олиб борилмоқда, жумладан: симметрик шифрлаш алгоритмлари акслантиришларини баҳолаш; мавжуд симметрик шифрлаш тармоқларини такомиллаштириш ва улар асосида янги алгоритмлар ишлаб чиқиш; шифрлаш алгоритмлари учун бардошли S-блоклар генерация қилиш усулларини яратиш; шифрлаш алгоритмлари бардошлигини замонавий криптотаҳлил усулларига баҳолаш; чизиқсизлиги юқори бўлган буль функциялар генерация қилиш усулларини яратиш; квант компютерларда ечилиши мураккаб математик масалалар асосида янги постквант асимметрик алгоритмлар яратиш; эллиптик эгри чизиқ асосида янги бардошли асимметрик шифрлаш алгоритмини яратиш; чекли майдонда дискрет логарифмлаш, мураккаб модул ва эллиптик эгри чизиқда дискрет логарифмлаш масалалари асосида янги бардошли ЭРИ алгоритмларини яратиш ҳамда улар дастурий воситалар мажмуини ишлаб чиқиш.

Муаммонинг ўрганилганлик даражаси. Симметрик шифрлаш алгоритмлари бардошликларини баҳолашда чизиқли, дифференциал, чизиқли-дифференциал, слайд, алгебраик, интеграл криптотаҳлил усуллари мавжуд бўлиб, улар назариялари мос равишда M.Matsui, E.Biham, A.Shamir, М.Хеллман, С.Лангфорд, А.Брюков, Д.Вагнер, К.Шеннон, N.Courtois, A.Klimov, J.Patarin, Л.Кнудсен каби олимлар томонидан яратилган.

Замонавий криптотаҳлил усуллари билан мавжуд симметрик шифрлаш алгоритмларини баҳолаш масалалари бир қатор олимлар томонидан тадқиқ қилинган, жумладан: ГОСТ 28147-89 шифрлаш алгоритми S-блоклари умумий криптографик талабларга А.Жуков, Н.Молдовян, А.Молдовян, дифференциал усулига Л.Бабенко, Е.Ищукова, чизиқли-дифференциал ва алгебраик усулларига Б.Абдурахимов, А.Саттаров, оддий ва такомиллашган слайд таҳлил усулларига Р.Алоев, Б.Ахмедов; Лай-Месси тармоғи асосидаги симметрик шифрлаш алгоритмлари чизиқли, дифференциал усулларига М.Арипов, Г.Туйчиев; параметрлар алгебраси асосида блокли симметрик шифрлаш алгоритми ва таҳлили П.Хасанов, М.Каримов, Х.Хасанов; ГОСТ Р 34.12-2015 стандарти Кузнечик алгоритми дифференциал ва чизиқли таҳлил усулларига Е.Ищукова, А.Марахимов, Г.Жураев; интеграл ва алгебраик усулларига Б.Абдурахимов, И.Бойқўзиев; ГОСТ Р 34.13-2015 стандарти имитомуҳофаза функцияси бардошликлари В.Гусев; O‘zDSt1105:2009 стандарт алгоритми интеграл ва алгебраик усулларига Б.Абдурахимов, О.Алланов ишларида баҳоланган.

Асимметрик алгоритмларни ишлаб чиқиш ҳамда улар бардошлигини баҳолаш масалалари қуйидаги олимлар илмий ишларида кўрилган, жумладан: криптографияда биринчи асимметрик алгоритм – симметрик шифрлаш алгоритми сеанс калитини биргаликда генерация қилиш протоколи У.Диффи, М.Хэллман; биринчи асимметрик шифрлаш ва электрон рақамли

имзо RSA ва EL-GAMAL алгоритмлари Р.Райвест, А.Шамир, Л.Адлеман ва Т.Жамол томонларидан; параметрлар алгебраси асосидаги асимметрик шифрлаш ва ЭРИ алгоритмлари М.Каримов, О.Ахмедова, М.Назарова; эллиптик эгри чизиқда дискрет логарифмлаш масаласига асосланган ЭРИ алгоритмлари ва крипто-протоколлар Н.Молдовян, А.Молдовян, Б.Изотов, Е.Дернова, Ю.Гурянов, Manoj Kumar Chande, Chend-Chi Lee, Chun-Ta Li, Nissa Mehibel, M'hamed Hamadouche; параметрлар алгебраси амаллари билан эллиптик эгри чизиқда дискрет логарифмлаш масаласига асосланган ЭРИ алгоритмлари П.Хасанов, Х.Хасанов, О.Ахмедова ишларида таклиф этилган. Эллиптик эгри чизиқ (a, b, p, G, [n]G) параметрларини бардошлилик талаблари бўйича генерация қилиш А.Ростовцев, Е.Маховенко, А.Буренкова, эллиптик эгри чизиқ асосидаги ЭРИ алгоритмларини бардошлиги таҳлили И.Горбенко, С.Збитнев, А.Поляков ишларида тадқиқ қилган. Шунингдек, мамлакатимизда ахборот хавфсизлиги ва криптография муаммолари масалаларида А.Кабулов, С.Ганиев, Р.Хамдамов, К.Керимов, Д.Иргашева, Д.Акбаров, З.Худайкулов ва бошқа олимлар томонидан илмий изланишлар олиб борилган.

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

Тадқиқотнинг мақсади бардошли симметрик, асимметрик шифрлаш ва электрон рақамли имзо алгоритмларини яратишдан иборат.

Тадқиқотнинг вазифалари:

бардошликлари оширилган симметрик шифрлаш алгоритмларини яратиш бўйича тавсиялар ишлаб чиқиш;

O'zDSt 1105:2009 ва ГОСТ Р 34.12-2015 стандарт алгоритмларини умумий криптографик талабларга баҳолаш;

эллиптик эгри чизиқ асосида бардошликлари оширилган асимметрик шифрлаш алгоритмлари математик моделларини яратиш;

дискрет логарифмлаш масаласи асосида бардошликлари оширилган электрон рақамли имзо алгоритмларини яратиш;

мураккаб модул асосида бардошликлари оширилган электрон рақамли имзо алгоритмларини яратиш;

эллиптик эгри чизиқда дискрет логарифмлаш мураккаблик асосида бардошликлари оширилган электрон рақамли имзо алгоритмларини яратиш.

Тадқиқотнинг объекти Симметрик шифрлаш алгоритмлари, криптотаҳлил усуллари, асимметрик шифрлаш ва электрон рақамли имзо алгоритмларидан иборат.

Тадқиқотнинг предмети Стандарт шифрлаш алгоритмларини лойиҳалаш босқичлари, O'zDSt 1105:2009 ва ГОСТ Р 34.12-2015 стандарт алгоритмларини умумий криптографик талабларга баҳолаш, эллиптик эгри чизиқда дискрет логарифмлаш мураккаблик масаласига асосланган асимметрик шифрлаш, чекли майдонда дискрет логарифмлаш, мураккаб

модулли, эллиптик эгри чизиқда дискрет логарифмлаш масалалари асосидаги электрон рақамли имзо алгоритмлари ташкил этади.

Тадқиқотнинг усуллари. Диссертацияда амалий криптография ва криптотаҳлил усуллари, алгебра ва сонлар назарияси, дискрет математика, ҳисоблаш математикаси, эҳтимоллар назарияси усулларидан ва объектга йўналтирилган дастурлаш технологияларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

стандарт симметрик шифрлаш алгоритмлари акслантиришларини балансланганлик, регулярлик, чизиқсизлик, коррелиацион иммуностлик, алгебраик иммунитетлик, чиқувчи битлар боғлиқсизлиги талабларига баҳолаш усули ишлаб чиқилган;

ГОСТ Р 34.12-2015 стандарт алгоритми S-блоклари бардошлиги чизиқсизлик қийматлари бўйича юқори ва O‘zDSt 1105:2009 алгоритми S-блоки бардошсизлиги исботланган;

O‘zDSt 1105:2009 стандарт алгоритми S-блоки учун параметрлар алгебраси амаллари ёрдамида юқори криптографик талабларни таъминловчи калитга боғлиқсиз чизиқсиз акслантириш ишлаб чиқилган;

маълумотни эллиптик эгри чизиқ нуқтаси сифатида ифодалаш ва эллиптик эгри чизиқ нуқтасини маълумот сифатида ифодалаш алгоритмларидан фойдаланиб, эллиптик эгри чизиқ асосида янги асимметрик шифрлаш алгоритми ишлаб чиқилган;

актив ҳужум усулига бардошли эллиптик эгри чизиқ асосида янги оптимал асимметрик шифрлаш алгоритми ишлаб чиқилган;

чекли майдонда дискрет логарифмлаш, эллиптик эгри чизиқда дискрет логарифмлаш мураккабликларига асосланган ва мураккаб модулли янги бардошли электрон рақамли имзо алгоритмлари ишлаб чиқилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

симметрик шифрлаш алгоритмлари акслантиришларини умумий криптографик талабларга баҳоловчи дастурий таъминот ишлаб чиқилган;

эллиптик эгри чизиқ асосида янги асимметрик шифрлаш алгоритмлари ишлаб чиқилган ҳамда дастурий таъминотлари яратилган;

турли математик мураккаблик асосида янги электрон рақамли имзо алгоритмлари криптографик бардошлиликлари исбот қилинган.

Тадқиқот натижаларининг ишончлилиги. Диссертацияда олинган тасдиқларнинг ишончлилиги унда математик мулоҳазаларнинг қатъийлиги, сонлар назарияси, дискрет математика, криптография ва криптотаҳлил назариясининг усулларидан фойдаланиб исботланганлиги, ҳисоблаш тажрибалари натижалари яратилган дастурлар мажмуи орқали таққосланганлиги билан асосланган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти таклиф этилган умумий криптографик талабларга текшириш усули, асимметрик шифрлаш ва электрон рақамли имзо алгоритмлари телекоммуникация тармоғи орқали узатилаётган маълумотнинг махфийлиги, симметрик шифрлаш алгоритми сеанс калитини

хавфсиз алмашиш ва муаллифликдан бош тортиш масалаларини ечиш учун фойдаланиш мумкинлиги билан изоҳланади.

Тадқиқотда натижаларнинг амалий аҳамияти умумий криптографик талабларга баҳолаш усули, асимметрик шифрлаш ва турли мураккабликдаги электрон рақамли имзо алгоритмлари криптотаҳлили усуллари ҳамда дастурлар мажмуи республикада миллий стандарт алгоритмларни қабул қилиш бўйича “Криптолойиҳа” танловларида тегишли методика сифатида, бардошлилиги юқори янги симметрик, асимметрик шифрлаш ва электрон рақамли имзо алгоритмларини ишлаб чиқиш, криптотаҳлил усулларига назарий ва амалий баҳолаш бўйича эксперт хулосалар беришга имкон бериши билан изоҳланади

Тадқиқот натижаларининг жорий қилиниши. Бардошли криптографик алгоритмлар яратиш усулларини ишлаб чиқишга оид илмий янгиликлар асосида:

стандарт симметрик шифрлаш алгоритмларини балансланганлик, регулярлик, чизиқсизлик, коррелиацион иммуностлик, алгебраик иммунитетлик, чиқувчи битлар боғлиқсизлиги талабларига баҳолаш усули, O‘zDSt 1105:2009, ГОСТ Р 34.12-2015 стандарт алгоритмлари S-блокларини баҳолаш натижалари, янги оптимал асимметрик шифрлаш алгоритми ахборотни криптографик муҳофаза қилиш дастурий ва аппарат-дастурий қурилмалар криптомодулларида маълумотларни ҳимоялашда қўлланилган (Ахборотни криптографик муҳофазалаш соҳасида Ваколатли органнинг 2021 йил 30 октябрдаги 20/5888-сонли маълумотномаси). Илмий натижаларнинг қўлланиши қурилмаларда симметрик шифрлаш алгоритмлари учун бардошли S-блокларни генерация қилишга, муҳофазаланмаган алоқа канали орқали шифрлаш сеанс калитларини етказиб беришга ва рухсати чекланган ахборотни ишончли ҳимоялаш механизмини ишлаб чиқишга имкон берган;

чекли майдонда дискрет логарифмлаш, эллиптик эгри чизиқда дискрет логарифмлаш мураккабликларига асосланган ва мураккаб модулли янги бардошли электрон рақамли имзо алгоритмлари «UNICON.UZ» ДУКда “Ўзбекистон Республикаси очиқ калитлар инфратузилмасининг хавфсизлик сервисларини такомиллаштириш усуллари ва воситаларини ишлаб чиқиш” лойиҳасида аутентификация масаласини ҳал этишда қўлланилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2022 йил 11 февралдаги 33-8/771 сонли маълумотномаси). Илмий натижаларнинг қўлланиши очиқ калитлар инфратузилмаси хавфсизлигини таъминлаш ва O‘zDSt 1105:2009 стандарт алгоритми учун таклиф этилган математик модел мазкур алгоритмнинг бардошлигини ошириш имконини берган;

янги оптимал асимметрик шифрлаш алгоритми ва O‘zDSt 1105:2009, ГОСТ Р 34.12-2015 стандарт алгоритмлари S-блокларини баҳолаш усуллари №Ф706-17-“Ахборот тизимларида биометрик-криптографик технологиялар қўлланишининг тадқиқи” грант лойиҳасида ахборот тизимларида узатилаётган маълумотларни ҳимоялашда фойдаланилган (Ахборот

технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2022 йил 11 февралдаги 33-8/771 сонли маълумотномаси). Илмий натижаларнинг қўлланиши асимметрик алгоритмни “шифрлаш-имзолаш” ёки “имзолаш-шифрлаш” схемалари ўрнида фойдаланишга имкон берган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 12 та, жумладан 6 та халқаро ва 6 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилиниши. Тадқиқот мавзуси бўйича жами 31 илмий иш чоп этилган, шулардан, Ўзбекистон Республикаси Олий аттестация комиссиясининг докторлик диссертациялари асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларда 19 та мақола, шундан 5 таси хорижий ва 14 таси республика журналларида нашр этилган. Илмий мақолаларнинг 2 таси халқаро Scopus базасида қайд этилган. Шунингдек, 2 та ЭҲМ учун яратилган дастурий воситаларни қайдлаш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, бешта боб, хулоса, адабиётлар рўйхати ва 10 та иловадан иборат. Диссертация ҳажми 184 бетни ташкил этган.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида ўтказилган тадқиқотларнинг долзарблиги ва зарурати, тадқиқотнинг республика фан ва технологиялари ривожлантиришнинг устувор йўналишларига мос келиши асосланган. Диссертация мавзуси бўйича чет элдаги илмий тадқиқотларнинг қисқача маълумоти ва муаммонинг ўрганилганлик даражаси келтирилган, тадқиқотнинг мақсади ва вазифалари, объект ва предметлари кўрсатилган, тадқиқотнинг илмий янгилиги ва амалий натижалари баён қилинган, олинган натижаларнинг илмий ва амалий аҳамияти очиб берилган, тадқиқот натижаларини амалиётга жорий қилиш, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Блокли симметрик стандарт алгоритмларни умумий криптографик талабларга баҳолаш»** деб номланган биринчи бобида симметрик шифрлаш стандарт алгоритмлари акслантиришларини умумий криптографик талабларга баҳолаш бўйича тавсия, O‘zDSt 1105:2009 стандарт шифрлаш алгоритми акслантиришларини, ГОСТ Р 34.12-2015 стандарти Магма ва Кузнечик алгоритмлари S-блокларини умумий криптографик талабларга текшириш бўйича олинган натижалари келтирилган.

Диссертация иши **1.1-параграфида** симметрик шифрлаш стандарт алгоритмлари акслантиришларини умумий криптографик талабларга баҳолаш математик асослари учун зарур тушунчалар баёни ҳамда янги таклиф этилган ёки мавжуд блокли симметрик стандарт шифрлаш алгоритми акслантиришларини умумий криптографик талабларга баҳолаш бўйича тавсиялар келтирилган.

Диссертация иши **1.2-параграфи** O‘zDSt 1105:2009 стандарт шифрлаш алгоритми Qo‘shBosqichKalit, Sur, BaytAlmash акслантиришлари умумий криптографик талаблар бўйича баҳоланган ва улар натижалари асосида BaytAlmash чизиқсиз акслантириш учун янги математик модел таклиф этилган. Мазкур бўлим бўйича олинган натижалар қуйида тасдиқлар формасида келтирилган.

Тасдиқ 1. O‘zDSt 1105:2009 стандарт алгоритми Qo‘shBosqichKalit (Holat, Ke) ва Sur (Holat, Ke) акслантиришлари учун умумий чизиқсизлик қиймати $N(\varphi) = 0$.

Тасдиқ 2. O‘zDSt 1105:2009 шифрлаш алгоритми иловасида келтирилган мисолга нисбатан *BaytAlmash* акслантириши регуляр, мос бул функция компоненталари чизиқсизлик қийматлари $N(f_1)=102$, $N(f_2)=106$, $N(f_3)=102$, $N(f_4)=102$, $N(f_5)=100$, $N(f_6)=106$, $N(f_7)=104$, $N(f_8)=98$ алгебраик чизиқсизлик қийматлари 7 га, умумий чизиқсизлик қиймати 92 га ва коррелиацион иммуностлик қиймати (даражаси) 0 га тенг.

Умумий криптографик талабларга тегишли назарияга мувофиқ**, с**аккиз аргументли баланслашган буль функциянинг максимал алгебраик чизиқсизлик даражаси 7 ва мантиқий чизиқсизлик даражаси 112 бўлиши лозим. Демак**,** O‘zDSt 1105:2009 стандарт иловасида келтирилган назорат мисолдаги *BaytAlmash* акслантириши *S-блок* жадвалини умумий криптографик талаблар бўйича текширишдан олинган натижалар, мазкур акслантиришнинг тўлиқ криптографик хусусиятларини очиб бермайди.

Шунинг учун мазкур акслантиришда (*D*, *R*, *L***)** учлик параметрлар қийматларига нисбатан яратилган дастурий таъминотдан фойдаланиб, *BaytAlmash* акслантириши ёрдамида шартли равишда 10 та ҳар-хил *S*-блок жадваллар генерацияси амалга оширилиб, умумий чизиқсизлик қийматлари бўйича қуйидагича натижалар олинди:

1-жадвал

10 та ҳар-хил S-блоклар ва улар умумий чизиқсизлик қийматлари

S-блоклар	**D**	**R**	**L**	***N* (*φ*) қиймати**
BaytAlmash – 1	37	54	2	0
BaytAlmash – 2	31	8	2	15
BaytAlmash – 3	33	8	6	0
BaytAlmash – 4	119	198	2	14
BaytAlmash – 5	49	54	3	0
BaytAlmash – 6	65	160	2	0
BaytAlmash – 7	81	164	5	0
BaytAlmash – 8	93	168	7	3
BaytAlmash – 9	131	172	11	15

BaytAlmash – 10	121	246	4	0

Тасдиқ 3. *BaytAlmash* акслантиришида номаълум калитдан генерация қилинган 1, 3, 5, 6, 7, 10 чи S – блокларда умумий чизиқсизлик қиймати $N(\varphi) = 0$ га, қолган 2, 4, 8, 9 чи S – блокларда $N(\varphi)$ - умумий чизиқсизлик қиймати мос равишда 15, 14, 3 ва 15 ларга тенг.

Демак, миллий стандарт алгоритмида махфий калитнинг турли вариантларида умумий чизиқсизлик қийматларини максимал (яъни 8 аргументли баланслашган буль функция учун 112) таъминлаб берувчи генераторлар тадбиқ этиш талаб этилади.

O‘zDSt 1105:2009 стандарт алгоритми *BaytAlmash* акслантиришига киритилиши лозим бўлган ўзгартириш сифатида қуйидаги математик формула таклиф этилади.

Тасдиқ 4. Агар O‘zDSt 1105:2009 стандарт шифрлаш алгоритми *BaytAlmash* акслантириши $BaytAlmash\ (x, z) = y$, $y = M^* (x@z)^{-1} + v$ математик модель ёрдамида генерация қилинса, у ҳолда мазкур акслантириш учун умумий чизиқсизлик қиймат $N(\varphi) = 112$ тенг бўлади.

Бу ерда M, v – фиксирланган матрица ва векторлар AES стандарт алгоритми *SubBytes* – акслантиришида келтирилган каби қийматлар, z – мастер калит бўлиб, $x, y, z \in GF(2^8)$ майдон элементлари, $^{-1}$ амали $GF(2^8)$ майдонда тескари элемент, @ - амали $GF(2^8)$ майдон элементлари бўлган 7 даражали кўпҳадларни «a» параметр бўйича кўпайтириш ва шу майдонда келтирилмайдиган 8-даражали (масалан: $x^8+x^6+x^5+x^3+1$) кўпҳад бўйича қолдиғини ҳисоблаш.

Диссертация иши **1.3-параграфида** ГОСТ Р 34.12-2015 стандарти Магма алгоритми S-блоклари умумий криптографик талаблар бўйича баҳоланган.

Тасдиқ 5. Магма алгоритми S_i – блоклари (i=1,…8) учун акслантиришлар регуляр, умумий чизиқсизлик қийматлари 4 га, алгебраик иммунитетлик даражалари (барча чиқувчи бул функциялар тенгламалар системасида 2 ва ундан юқори даражали тенгламалар мавжуд) 2 га, чиқувчи битлар боғлиқ-сизлиги тамойили (BIC) қийматлари 0 га тенг.

Тасдиқ 6. Магма алгоритми S_i – блоклари (i=1,…8) бул функция компоненталари чизиқсизлик қийматлари $N(f_1) = 4$, $N(f_2) = 4$, $N(f_3) = 4$, $N(f_4) = 4$, барча бул функциялари учун корреляцион иммуностлик даражалари 0 га ва алгебраик чизиқсизлик даражалари қийматлари эса қуйидагиларга тенг:

S_1, S_2, S_5, S_7: $deg(f_1)=2$, $deg(f_2)=3$, $deg(f_3)=3$, $deg(f_4)=3$.

S_3, S_4, S_6, S_8: $deg(f_1)=3$, $deg(f_2)=3$, $deg(f_3)=3$, $deg(f_4)=3$.

Диссертация иши **1.4-параграфида** ГОСТ Р 34.12-2015 стандарти Кузнечик алгоритми S-блоки умумий криптографик талаблар бўйича баҳоланган.

Тасдиқ 7. Кузнечик алгоритми S – блоки учун акслантириш регуляр, умумий чизиқсизлик қиймати 100 га, алгебраик иммунитетлик даражаси (барча чиқувчи бул функциялар тенгламалар системасида уч ва ундан юқори

даражали тенгламалар мавжуд) 3га, чиқувчи битлар боғлиқсизлиги тамойили (BIC) қиймати 0 га тенг.

Тасдиқ 8. Кузнечик алгоритми S – блоки бул функция компонента-ларининг чизиқсизлик қийматлари мос равишда: $N(f_1)=104$, $N(f_2)=106$, $N(f_3)=116$, $N(f_4)=104$, $N(f_5)=110$, $N(f_6)=106$, $N(f_7)=102$, $N(f_8)=104$ барча бул функциялари учун корреляцион иммуностлик даражаси 0 га ва алгебраик чизиқсизлик даражаси қийматлари 7 га тенг.

Турли шифрлаш алгоритмлари S – блокларини умумий криптографик талабларга баҳолаш натижасида олинган қийматларни ўзаро солиштириш қуйидаги 2-жадвалда келтирилган.

2 -жадвал.

Алгоритмлар S – блокини умумий талаблар бўйича баҳолаш натижалари

Умумий криптографик талаблар	**Магма**	**ГОСТ 28147-89**	**Кузнечик**	**AES**
	S – блоклари $GF(2^4)\to GF(2^4)$	S – блоклари $GF(2^4)\to GF(2^4)$	S – блоки $GF(2^8)\to GF(2^8)$	S – блоки $GF(2^8)\to GF(2^8)$
Балансланган	+	+	+	+
Регулярлик	+	+	+	+
$\deg(f)$	2 ёки 3	3	7	7
$N(f)$	4	2 ёки 4	102-116	112
$N(\varphi)$	4	2	100	112
$CI(f)$	0	0	0	0
$AI(S)$	2	2	3	2
$BIC(S)$	0	0	0	0

Диссертациянинг **«Эллиптик эгри чизиқ асосида янги асимметрик шифрлаш алгоритмини яратиш»** деб номланган иккинчи бобида замонавий асимметрик шифрлаш алгоритмлари математик асослари, эллиптик эгри чизиқга асосланган асимметрик шифрлаш алгоритмини яратиш билан боғлиқ масалалар, маълумотларни эллиптик эгри чизиқ нуқталари сифатида ифодалаш алгоритмлари ва эллиптик эгри чизиқ асосидаги янги асимметрик шифрлаш алгоритми математик модели ҳамда ундан олинган натижалар келтирилган.

Диссертация иши **2.1-параграфида** асимметрик алгоритмларни эллиптик эгри чизиқларга ўтказиш билан боғлиқ масалалар математик асослари баён қилинган.

Диссертация иши **2.2-параграфида** маълумотларни эллиптик эгри чизиқ нуқталари кўринишда ифодалаш алгоритми келтирилган.

Маълумотни эллиптик эгри чизиқ асосидаги асимметрик алгоритм билан шифрлаш жараёнида қуйидаги муаммолар пайдо бўлади:

Жумладан шифрлаш жараёнида *M* маълумот қиймати ҳам эллиптик эгри чизиқнинг нуқтаси бўлиши керак. Бироқ амалиётда маълумот ҳар доим ҳам эллиптик эгри чизиқнинг нуқтаси бўлиш шартини бажармайди. Шунинг учун мазкур муаммо ечими сифатида қуйидаги ёндашувлар таклиф этилган.

1-ёндашув. Шифрланувчи маълумотни ифодалашда ишлатиладиган белгилар (ASC II коди) танланган эллиптик эгри чизиққа нисбатан нуқталар сифатида акс эттирилади.

Ушбу ёндошув камчилиги шифрловчи ва очиқ матнга ўгирувчи томонларга маълум бўлган ASC II коди бўйича эллиптик эгри чизиқ нуқталарини ифодаловчи жадвалнинг мавжуд бўлиши ҳисобланади.

2-ёндашув. Шифрланувчи маълумот тегишли узунликларга бўлиниб, унинг блоклари тегишли алгоритм ёрдамида эллиптик эгри чизиқ нуқтаси бўлиш шарти бўйича амалга оширилади.

Диссертация ишида янги асимметрик шифрлаш алгоритмини ишлаб чиқишда 2-ёндошувдан фойдаланилган.

Қуйида шифрланиши лозим бўлган m маълумот блокларини эллиптик эгри чизиқга тегишли M (x,y) нуқта сифатида ифодалаш ва уни m маълумот кўринишига ўтказиш алгоритмлари келтирилган.

Маълумот блокларини эллиптик эгри чизиқга тегишли нуқта сифатида ифодалаш алгоритми қуйидагича:

1. Санагич $i = 0$ қилиб ўрнатилади, $p' = p\ div\ 2^{\pi-\mu}$ ҳисобланади p' ва m_i ларни иккилик сон сифатида солиштирилади (div – бутун қисмини олиш операцияси). Агар $p' > m_i$ бўлса, 2 – қадамга, акс ҳолда 3 – қадамга ўтилади.
2. Агар $i < 2^{\rho}$ бўлса, иккилик қиймати i га тенг бўлган ρ – битли r сатр шакллантирилади ва 7 – қадамга ўтилади. Акс ҳолда “Эллиптик эгри чизиқ нуқтаси мавжуд эмас” деган хабар чиқади.
3. Агар $i < 2^{\rho-1}$ бўлса, иккилик қиймати i га тенг $\rho - 1$ битли r сатр шакллантирилади ва 4 – қадамга ўтилади. Акс ҳолда “ Эллиптик эгри чизиқ нуқтаси мавжуд эмас” деган хабар чиқади.
4. x - ўзгарувчига $m_i||r$ ўзлаштирилиб, $w = (x^3 + ax + b) \bmod p$ қиймат ҳисобланади.
5. Лежандр символи $\lambda = (\frac{w}{p})$ қиймати ҳисобланади. Агар $\lambda = -1$ бўлса, санагич биттага оширилади ($i \leftarrow i + 1$) ва 3 – қадамга ўтилади, акс ҳолда 6 – қадамга ўтилади.
6. Илдизнинг иккита қиймати ҳисобланади $y_{1,2} = \pm\sqrt{w} \pmod p$, бу ерда $y_{1,2} \in \{1, 2, \dots, p - 1\}$, $y_{1,2}$ ларнинг кичик қиймати y га ўзлаштирилади ва 10 – қадамга ўтилади.
7. x - ўзгарувчига $m_i||r$ ўзлаштирилиб, $w = (x^3 + ax + b) \bmod p$ қиймат ҳисобланади.

8. Лежандр символи $\lambda = (\frac{w}{p})$ қиймати ҳисобланади. Агар $\lambda = -1$ бўлса, санагич биттага оширилади $(i \leftarrow i + 1)$ ва 2 – қадамга ўтилади, акс ҳолда 9 – қадамга ўтилади.

9. Илдизнинг иккита қиймати: $y_{1,2} = \pm\sqrt{w}\,(\mathrm{mod} p)$ ҳисобланади, бу ерда $y_{1,2} \in \{1, 2, \dots, p-1\}$, $y_{1,2}$ қийматлар каттаси y - ўзгарувчига ўзлаштирилади ва 10 – қадамга ўтилади.

10. Ҳосил бўлган (x,y) координаталар жуфтлиги m маълумот эллиптик эгри чизиққа тегишли M (x,y) нуқтаси деб эълон қилинади.

Эллиптик эгри чизиқ нуқтаси сифатида ифодаланган M (x,y) нуқтани қуйидаги алгоритм ёрдамида маълумот кўринишига ўтказиш амалга оширилади.

1. $w = (x^3 + ax + b) \bmod p$ қиймат ҳисобланади.
2. $y_{1,2} = \pm\sqrt{w} \bmod p$ ҳисобланади ва $y_1 < y_2$ шарт текширилади, бунда $y_1, y_2 \in \{1,2, \dots, p-1\}$.
3. Агар $y = y_1$ бўлса, $m = x\ div\ 2^{p-1}$, акс ҳолда $m = x\ div\ 2^p$ нинг қиймати олинади.

Диссертация иши **2.3-параграфида** берилган m маълумот блокларини эллиптик эгри чизиқга тегишли M (x,y) нуқта сифатида ифодалаш ҳамда эллиптик эгри чизиқ нуқтасини m маълумот кўринишига ўтказиш алгоритмларидан фойдаланиб, эллиптик эгри чизиқ асосида янги асимметрик шифрлаш алгоритми математик модели таклиф этилган.

Асимметрик алгоритмни аниқлаш учун шифрлаш ва маълумотларни дастлабки матнга ўгириш жараёнида қўлланиладиган асосий математик объектларни баён этиш зарур. Қуйида асимметрик алгоритм объектларига қўйиладиган асосий математик таърифлар ва талаблар белгиланган.

Айтайлик, асимметрик шифрлаш алгоритми: $y^2 \equiv x^3 + ax + b \pmod p$ формула билан аниқланган эллиптик эгри чизиқ ва қуйидаги параметрлардан фойдаланади:

a) p туб сон $p>2^{255}$ тенгсизликни қаноатлантирувчи, эллиптик эгри чизиқ модули. Ушбу соннинг юқори чегараси асимметрик алгоритмни муайян амалга ошириш жараёнида белгиланади;

b) ўзининг $J(E)$ инварианти ёки $a,b \in F_p$ коэффициентлари билан берилган E эллиптик эгри чизиқ;

d) n туб сон – қуйидаги шартлар бажарилган E эллиптик эгри чизиқ нуқталари группаси циклик қисм группасининг тартиби:

$$\begin{cases} w = l * n, l \in Z, l \geq 1 \\ 2^{254} < n < 2^{256} \end{cases}$$

e) $G(x_0,y_0)$, $[n]G=0$ ва $G \neq 0$ тенгликларни қаноатлантирувчи E эллиптик эгри чизиқнинг (x_0,y_0) координатали базавий нуқтаси;

Асимметрик шифрлаш алгоритми параметрларига қуйидаги талаблар қўйилади:

a) барча бутун *i=1, 2…, B* сонлар учун $p^i \neq 1 \pmod n$ шарт бажарилиши лозим, бу ерда, *B* учун $B \geq 31$ тенгсизлик бажарилади;

b) $w \neq p$ тенгсизлик бажарилиши лозим;

d) эгри чизиқ инварианти $J(E) \neq 0$ ёки 1728 шартларни қаноатлантириши лозим.

Асимметрик шифрлаш алгоритмининг ҳар бир фойдаланувчиси қуйидаги шахсий калитларга эга бўлиши керак:

a) асимметрик алгоритм ёпиқ калити d, $0<d<n$ тенгсизликни қаноатлантирувчи бутун сон;

b) асимметрик алгоритм очиқ калити Q – (x, y) координатали, $[d]G=Q$ тенгликни қаноатлантирувчи эллиптик эгри чизиқ нуқтаси.

Янги таклиф этилаётган асимметрик шифрлаш алгоритми математик модели қуйидаги қадамлар кетма-кетлигидан иборат.

Шифрланиши лозим бўлган m маълумот $\rho = \pi - \mu = 16$ шарт асосида μ битли блокларга ажратилади ($m = \{m_1, m_2, \dots, m_i\}$, $|m_i| = \mu$ бит, бу ерда, p туб сони разряди π битга тенг).

I. Маълумотни шифрлаш жараёни.

1. Маълумотни шифрловчи томон k сонни $0 < k < n$ ораликдан танлайди ва у фақат ўзигагина маълум сон.

2. $C_1 = [k]G$, $R = [k]Q$ эллиптик эгри чизиқ нуқталари ҳисобланади.

3. Шифрланувчи маълумот эллиптик эгри чизиқ нуқтаси бўлиш шартига текширилади. Агар маълумот эллиптик эгри чизиқ нуқтаси бўлмаса, 7 – қадамга, акс ҳолда қуйидаги ҳисоблашлар бажарилади.

4. Шифрланувчи M (x,y) нуқта x абциссасидан фойдаланиб, y_1, y_2 нинг қиймати ҳисобланади. Агар $y = \min(y_1, y_2)$ бўлса, 6 – қадамга ўтилади, акс ҳолда қуйидаги ҳисоблашлар амалга оширилади.

5. $C_2 = M + R$ эллиптик эгри чизиқ нуқтаси ҳисобланади ва $q = 3$ қиймат учун $t = x_{C_2} || q$ бажарилади ҳамда 8 – қадамга ўтилади (бу ерда $|q| \rightarrow 2$ бит).

6. $C_2 = M + R$ эллиптик эгри чизиқ нуқтаси ҳисобланади ва $q = 1$ қиймат учун $t = x_{C_2} || q$ бажарилади ҳамда 8 – қадамга ўтилади (бу ерда $|q| \rightarrow 2$ бит).

7. $C_2 = M \cdot R = (x_{C_2}, y_{C_2})$ ҳисобланади (ёки $x_{C_2} = m_i \oplus x_R$ формула) ва $q = 0$ қиймат учун $t = x_{C_2} || q$ бажарилади ҳамда 8 – қадамга ўтилади (бу ерда $|q| \rightarrow 2$ бит).

8. $C = \{C_1, t\}$ шифр матн ҳосил бўлади.

II. Шифр матнни очиқ матнга ўгириш жараёни.

1. $U(x_u, y_u) = [d]C_1$ ҳисобланади.
2. $q = 0$ шарт бажарилса 8 – қадамга, акс ҳолда 3-қадамга ўтилади.
3. Агар $q = 3$ бўлса, 4 – қадамга, $q = 1$ бўлса, 6 – қадамга ўтилади.
4. $w = x_{C_2}^3 + a x_{C_2} + b \pmod p$.

5. $y_{1,2} = \pm\sqrt{w} \pmod p$ ҳисобланади ва $y = \max(y_1, y_2)$ танланиб, 9 – қадамга ўтилади.

6. $w = x_{C_2}^3 + ax_{C_2} + b \pmod p$ ҳисобланади.

7. $y_{1,2} = \pm\sqrt{w} \pmod p$ ҳисобланади ва $y = \min(y_1, y_2)$ танланиб, 9 – қадамга ўтилади.

8. $M = \frac{x_{C_2}}{x_U}$ очиқ матн ҳисобланади.

9. $M = (x_{C_2}, y) - U(x_u, y_u)$ эллиптик эгри чизиқ нуқтаси ҳисобланади.

10. $M(x,y)$ нуқта m маълумот кўринишда ифодалаш алгоритми ёрдамида очиқ матнга ўтказилади.

Таклиф этилган асимметрик шифрлаш алгоритми учун қуйидаги теорема исбот қилинган.

Теорема 1. Эллиптик эгри чизиққа асосланган маълумотни шифрлаш 8 та қадамини ва шифрматнни очиқ матнга ўгириш 10 та қадамини ўз ичига олган асимметрик шифрлаш алгоритми коррект.

Диссертация иши **2.4-парагарфида** эллиптик эгри чизиқга асосланган янги асимметрик шифрлаш алгоритмидан олинган натижалар таҳлили келтирилган.

Эллиптик эгри чизиқ асосидаги асимметрик шифрлаш алгоритмида маълумотларнинг хотирадан эгаллаган ҳажми бўйича натижалар 3-жадвалда берилган.

3-жадвал.

Ҳажм бўйича олинган натижалар

Маълумот узунлиги (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Нуқта кўринишида ифодалаш (байт)	1 276 766	6 429 202	12 841 346	128 510 799
Шифрлаш жараёни (байт)	1 275 581	6 378 273	12 757 262	127 572 670
Очиқ матнга ўгириш жараёни (байт)	1 276 766	6 429 202	12 841 346	128 510 799
Маълумотни тиклаш (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Шифр матн ҳажми ўзгариши (%)	21,65 % ортди	21,66 % ортди	21,66 % ортди	21,66 % ортди

Эллиптик эгри чизиқ асосидаги асимметрик шифрлаш алгоритмида маълумотларнинг шифрлаш ва очиқ матнга ўгириш жараёни учун сарфланган вақти қуйидаги жадвалда келтирилган.

4-жадвал.

Шифрлаш ва очиқ матнга ўгириш учун сарфланган вақтлар

Маълумот узунлиги (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Нуқта кўринишида	20	100	199	1998

ифодалаш учун сарфланган вақт (секунд)				
Шифрлаш жараёни учун сарфланган вақт (секунд)	122	612	1223	12235
Очиқ матнга ўгириш жараёни учун сарфланган вақт (секунд)	118	591	1179	11807
Маълумотни тиклаш учун сарфланган вақт (секунд)	5	25	50	499
Умумий сарфланган вақт (минут)	$4\frac{5}{12}$ мин	$22\frac{2}{15}$ мин	$44\frac{11}{60}$ мин	$442\frac{19}{60}$ мин

Эллиптик эгри чизиқга асосланган асимметрик шифрлаш алгоритмидан олинган натижаларни факторизация масаласига асосланган RSA, дискрет логарифмлаш масаласига асосланган Эл-Гамал стандарт асимметрик шифрлаш алгоритмлари билан солиштириш мақсадида тегишли дастурий таъминотлар яратилди. Олинган натижалар бўйича қуйидаги тасдиқлар ўринли.

Тасдиқ 9. Таклиф этилган эллиптик эгри чизиқ асосидаги шифрлаш алгоритми RSA алгоритмига нисбатан хотирадан 16,65 % кўп ҳажм эгаллайди, тезлиги бўйича 2,2 марта тез ҳисобланади.

Тасдиқ 10. Таклиф этилган эллиптик эгри чизиқ асосидаги шифрлаш алгоритми Эл – Гамал алгоритмига нисбатан хотирадан 78,35 % кам ҳажм эгаллайди, тезлиги 4,65 марта тез ҳисобланади.

Диссертациянинг **«Эллиптик эгри чизиқ асосида бардошлиги оширилган асимметрик шифрлаш алгоритмини яратиш»** деб номланган учинчи бобида замонавий асимметрик шифрлаш алгоритмларига актив криптоҳужум усули қўлланиши билан боғлиқ масалалар, актив криптоҳужум усулига бардошли янги оптимал асимметрик шифрлаш алгоритми математик модели ва ундан олинган натижалар таҳлили баён қилинган.

Диссертация иши **3.1-параграфида** замонавий асимметрик шифрлаш алгоритмларига актив криптоҳужум усули қўлланиши билан боғлиқ масалалар баён қилинади.

Таъриф. Махфий маълумот узатиш жараёнини узиб қўйиш, модификациялаш, қалбаки шифр маълумотлар тайёрлаш каби ҳатти-ҳаракатлар актив ҳужум дейилади.

Бугунги кунда замонавий асимметрик криптография фанида “Танлаб олинган очиқ матн асосидаги ҳужум(chosen-plaintext attack-CPA)”, “Танлаб олинган шифр матн асосидаги ҳужум(chosen-ciphertext attack-CCA)”, “Адаптив танлаб олинган шифр матнлар асосидаги ҳужум (adaptive chosen-ciphrtext attack-CCA2)” каби актив криптоҳужум усулларидан келиб чиқиб, асимметрик криптотизимлар бардошли бўлиши учун асосий талаблар ишлаб чиқилган. Ўтказилган таҳлил натижаларига кўра қуйидаги тасдиқ ўринли.

Тасдиқ 11. RSA стандарт алгоритми актив криптоҳужум усулига бардошсиз.

Мазкур тасдиқ нафақат RSA стандарт алгоритмига балки барча асимметрик шифрлаш алгоритмлари учун ўринли. Жумладан, диссертация иши 2-бобида таклиф этилган эллиптик эгри чизиқда дискрет логарифмлаш мураккаблик масаласига асосланган асимметрик шифрлаш алгоритми актив криптоҳужум усулларига бардошсиз ҳисобланади. Натижада мазкур алгоритмнинг оптимал вариантини ишлаб чиқиш зарурати келиб чиқади.

Диссертация иши **3.2-параграфида** янги оптимал асимметрик шифрлаш алгоритми математик модели ишлаб чиқилди.

Бугунги кунда RSA стандарт алгоритми амалиётда классик адабиётларда келтирилган қадамларига тўлдириш схемаси қўшилган асимметрик RSA-OEP алгоритмидан фойдаланилади.

Мазкур ҳолат 2-бобда таклиф этилган эллиптик эгри чизиқ асосидаги асимметрик шифрлаш алгоритмини такомиллаштириш заруратини келтириб чиқаради. Қуйида эллиптик эгри чизиқ ёрдамида маълумотни шифрлаш ва дастлабки матнга ўгириш қадамлари учун оптимал асимметрик шифрлаш алгоритми келтирилган.

Алгоритм шифрлаш жараёни.

M – дастлабки маълумотни шифрловчи томон фақат ўзига маълум бўлган k – сонни $0<k<n$ ораликдан тасодифий танлайди. Ундан фойдаланиб $C_1=[k]G$ ва $R=[k]Q$ каби эллиптик эгри чизиқ нуқталари ҳисобланади.

Берилган M – маълумот $\mu = \pi - k_0 - k_1 - 16$ шарт асосида μ битли блокларга ($M = \{m_1, m_2, ..., m_v\}$, $|m_i| = \mu$ бит) бўлинади.

Ҳар бир $|m_i| = \mu$ бит узунликдаги очиқ матн блоки κ_0 та ноллар билан тўлдирилади ва қуйидаги кетма-кетликда алоҳида шифрланади.

1. Узунлиги k_1=128 бит бўлган тасодифий l – маълумот ҳосил қилинади.
2. $S_1 = (m_i \| 0^{k_0}) \oplus Hesh1(l)$ ҳисобланади.
3. $S_2 = l \oplus Hesh2(S_1)$ ҳисобланади.
4. $S = S_1 \| S_2$ маълумот ҳосил қилинади.
5. S – маълумот эллиптик эгри чизиқ $M(x,y)$ нуқтаси бўлиши шарти текширилади. Агар маълумот эллиптик эгри чизиқ нуқтаси бўлмаса, 11-қадамга ўтилади.
6. $M(x,y)$ нуқта x – координатасидан фойдаланиб $w = (x^3 + ax + b) \bmod p$ қиймат ҳисобланади.
7. $y_{1,2} = \pm\sqrt{w} \pmod p$ қийматлар ҳисобланади.
8. Агар $y = \min(y_1, y_2)$ бўлса, 10-қадамга ўтилади.
9. q – ўзгарувчига 3 қиймат ўзлаштирилади (q=3) ҳамда $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \| q$ ҳисобланади ва 12-қадамга ўтилади (бу ерда $|q|$=2 бит).
10. q – ўзгарувчига 1 қиймат ўзлаштирилиб (q=1), $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \| q$ ҳисобланади ва 12-қадамга ўтилади.

11. q – ўзгарувчига 0 қиймат ўзлаштирилади (q=0) ҳамда $x_{C_2} = S \oplus x_R$ $t = x_{C_2} \| q$ ҳисобланади.

12. E_i={$C_1(x,y),t$} – шифрматн блоки сифатида эълон қилинади.

Шифрланган E_i (E_i={$C_1(x,y),t$}) маълумот блокларини дастлабки матнга ўгириш жараёни

1. $U(x_u, y_u) = [d]C_1$ эллиптик эгри чизиқ нуқтаси ҳисобланади.

2. Агар q=0 бўлса, $S = x_{C_2} \oplus x_U$ ҳисобланади ва 10-қадамга ўтилади.

3. $w = \left(x_{C_2}^3 + ax_{C_2} + b\right) \bmod p$ ҳисобланади.

4. $y_{1,2} = \pm\sqrt{w} \pmod p$ ҳисобланади.

5. Агар q=3 бўлса, 7-қадамга ўтилади.

6. $y = \min(y_1, y_2)$ ҳисобланади ва 8-қадамга ўтилади.

7. $y = \max(y_1, y_2)$ ҳисобланади.

8. $M(x,y) = \left(x_{C_2}, y\right) - U\left(x_U, y_U\right)$ эллиптик эгри чизиқ нуқтаси ҳисобланади.

9. $M(x,y)$ нуқта S – маълумот кўринишида ифодаланади.

10. S – маълумотнинг дастлабки $\mu + k_0$ та бити S_1 га, охирги k_1 та бити S_2 га юкланади (яъни: $S_1||S_2=S$).

11. $l = S_2 \oplus Hesh2\left(S_1\right)$ ҳисобланади.

12. $Sm = S_1 \oplus Hesh1\left(l\right)$ ҳисобланади.

13. Агар Sm – маълумотнинг сўнгги k_0 та бит қиймати нолга тенг бўлса, у ҳолда "*маълумот ҳақиқий*" бўлиб, Sm – маълумотнинг дастлабки μ та бити m_i – очиқ матн блоки сифатида, акс ҳолда "*маълумот соҳта*" (қалбаки) деб эълон қилинади.

Бу ерда, μ – сони m_i маълумотнинг битлардаги узунлигини аниқловчи символ, p – туб сон, p>3, π – берилган p туб сон разрядини аниқловчи символ; k_0, k_1 – натурал сонлар, $Hesh1$ ва $Hesh2$ – хэш-қиймат узунликлари мос равишда $\mu + k_0$ ва k_1 бит бўлган бардошли хэш-функциялар.

Таклиф этилган янги оптимал асимметрик шифрлаш алгоритми учун қуйидаги теорема исбот қилинган.

Теорема 2. Эллиптик эгри чизиққа асосланган маълумотни шифрлаш 12 та қадамни ва шифрматнни очиқ матнга ўгириш 13 та қадамини ўз ичига олган оптимал асимметрик шифрлаш алгоритми коррект ва актив криптоҳужум усулига бардошли.

Диссертация иши **3.3-параграфида** эллиптик эгри чизиққа асосланган оптимал асимметрик шифрлаш алгоритмидан олинган натижалар таҳлили баён қилинган.

Эллиптик эгри чизиқ асосидаги оптимал асимметрик шифрлаш алгоритмининг хотирадан эгаллаган ҳажми ва сарфланган вақт параметрлари бўйича баҳолаш натижалари 5 ва 6-жадвалларда келтирилган.

5-жадвал.

Ҳар хил узунликларда хотирадан эгаллаган ҳажм

Маълумот узунлиги (байт)	37982	75964	151928	1 671 208
Маълумотни тўлдириш (байт)	93504	187008	374016	4113792
Нуқта кўринишида ифодалаш (байт)	113671	227307	454671	5 001 086
Шифрлаш жараёни (байт)	113756	227547	455026	5005191
Очиқ матнга ўгириш жараёни (байт)	113671	227307	454671	5 001 086
Нуқта кўриниши-дан маълумотни тиклаш (байт)	93504	187008	374016	4113792
Маълумотни қайта тиклаш (байт)	37982	75964	151928	1 671 208
Шифр матн ҳажми ўзгариши (%)	199 %	199 %	199 %	199 %

6-жадвал.

Ҳар хил узунликларда сарфланган вақт

Маълумот узунлиги (байт)	37982	75964	151928	1 671 208
Маълумотни тўлдириш учун сарфланган вақт (секунд)	0,639	1,294	2,589	27,728
Нуқта кўринишида ифодалаш учун сарфланган вақт (секунд)	1,778	3,588	7,208	77,782
Шифрлаш жараёни учун сарфланган вақт (секунд)	10,281	20,561	41,06	451,433
Очиқ матнга ўгириш жараёни учун сарфланган вақт (секунд)	10,281	21,092	41,356	451,83
Нуқта кўринишидан маълумотни тиклаш учун сарфланган вақт (секунд)	0,421	0,827	1,654	18,665
Маълумотни тўлдириш схемасидан фойдаланиб тиклаш	0,624	1,263	2,48	27,22
Умумий сарфланган вақт (секунд)	24,413	48,625	96,347	1054,037

Дастурий таъминот ёрдамида эллиптик эгри чизиқ асосидаги оптимал асимметрик шифрлаш алгоритмидан олинган натижалар RSA оптимал

шифрлаш алгоритми натижалари билан солиштирилди. Олинган натижалар асосида қуйидаги тасдиқлар ўринли.

Тасдиқ 12. RSA оптимал алгоритми RSA алгоритмига нисбатан хотирадан 150,79 % кўп ҳажм эгаллайди, вақт бўйича 2,4 марта секин ишлайди.

Тасдиқ 13. Эллиптик эгри чизиқ асосидаги оптимал шифрлаш алгоритми эллиптик эгри чизиқ асосидаги шифрлаш алгоритмига нисбатан хотирадан 177,35 % кўп ҳажм эгаллайди, тезлиги бўйича 2,5 марта секин ишлайди.

Тасдиқ 14. Таклиф этилган эллиптик эгри чизиқ асосидаги оптимал шифрлаш алгоритми RSA оптимал шифрлаш алгоритмига нисбатан хотирадан 40% кўп ҳажм эгаллайди, лекин тезлиги бўйича 2,4 марта тез ишлайди.

Диссертациянинг **«Дискрет логарифмлаш ва мураккаб модул асосида бардошликлари оширилган электрон рақамли имзо алгоритмларини яратиш»** деб номланган тўртинчи бобида электрон рақамли имзо алгоритмлари (ЭРИ) ни қалбакилаштириш усуллари, чекли майдонда дискрет логарифмлаш, мураккаб модул (факторизация ва дискрет логарифмлаш) масалаларига асосланган янги ЭРИ алгоритмлари таклиф этилган ва улар криптотаҳлили жараёнлари келтирилган.

Бунги кунда замонавий ЭРИ алгоритмларини яратиш таҳлиллари натижасига мувофиқ уларни қалбакилаштиришнинг қуйидаги учта усули мавжуд:

- имзода фойдаланилган математик мураккабликни самарали ечиш орқали;
- хэш қийматни коллизияга учратиш орқали;
- имзо алгоритмида йўл қўйилган хатоликлардан фойдаланиш орқали.

Диссертация иши **4.1-параграфида** ЭРИ алгоритмларини қалбакилаштириш усуллари асосида дискрет логарифмлаш мураккаблигига асосланган бардошсиз ЭРИ алгоритмларидан олинган натижалар баён қилинган.

Айтайлик, имзони шакллантириш ва текширишда x ёпиқ ва y очиқ калитлар орасидаги боғланиш $y = g^x \bmod p$ чекли майдонда дискрет логарифмлаш масаласи мураккаблиги асосида берилган бўлсин. У ҳолда мазкур параграфда кўриб чиқилган ЭРИ алгоритмлари таҳлилига мувофиқ, қуйидагилар исбот қилинди.

Теорема 3. Агар k имзо эгасига маълум бирор $(0 < k < p)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = (g^k \bmod p),\ s=(k-hx)r^{-1}(\bmod p-1)$$

формулалар, имзони текшириш $r=y^h g^{rs}(\bmod p)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект, лекин бардошсиз ҳисобланади.

Теорема 4. Агар k имзо эгасига маълум бирор $(0 < k < p)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = g^k(\bmod p),\ s = (k-h)r^{-1}x^{-1}(\bmod p-1)$$

формулалар, имзони текшириш $r = g^h y^{rs} (\mathrm{mod}\, p)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект, лекин бардошсиз ҳисобланади.

Диссертация иши **4.2-параграфида** чекли майдонда дискрет логарифмлаш муаммосига асосланган янги ЭРИ алгоритмларини яратиш ва улар криптотаҳлили масалалари келтирилган.

Теорема 5. Агар k имзо эгасига маълум бирор $(0 < k < q)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = (g^k (\mathrm{mod}\, p))(\mathrm{mod}\, q),\ s = k^{-1}(xr + H(M))(\mathrm{mod}\, q),\ a_1 = [\, H(M)\, s^{-1} / q\,],$$

$$a_2 = [\, r\, s^{-1} / q\,],\ a_3 = [s^{-1} / q],\ \alpha \equiv (g^{q(a_3(H(M)+xr)+a_1+a_2 x)} \bmod p) \bmod q$$

формулалар ёрдамида, имзони текшириш $u = \alpha (g^{u_1} y^{u_2} \mod p)(\mathrm{mod}\, q)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s, α) имзо коррект, лекин бардошсиз ҳисобланади.

Бу ерда, $y = g^x (\mathrm{mod}\, p)$, $u_1 = (\mathrm{H(M)}\ w) \bmod q$, $u_2 = (r\ w) \bmod q$, $w = s^{-1} (\mathrm{mod}\, q)$ ва p, q, g - параметрлар DSA ЭРИ алгоритмидаги каби генерация қилинади, H(M) - берилган M маълумот хэш қиймати.

Теорема 6. Агар k имзо эгасига маълум бирор $(0 < k < q)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = (g^k (\mathrm{mod}\, p))(\mathrm{mod}\, q),\ s = k^{-1}(xr + H(M))(\mathrm{mod}\, q),\ a_1 = [\, \mathrm{H(M)}\, s^{-1} / \mathrm{q}\,]$$

$$\alpha = q(a_3(\mathrm{H(M)} + xr) + a_1 + a_2 x),\ ,\ a_2 = [\, r\, s^{-1} / q\,],\ a_3 = [s^{-1} / q]$$

формулалар ёрдамида, имзони текшириш $u = g^{\alpha} (g^{u_1} y^{u_2} \mod p)(\mathrm{mod}\, q)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s, α) имзо коррект ва бардошли ҳисобланади.

Бу ерда, y, u_1, u_2, H(M) ва p, q, g – параметрлар теорема 5 каби аниқланган.

Теорема 7. Агар k имзо эгасига маълум бирор $(0 < k < q)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = (g^k (\mathrm{mod}\, p))(\mathrm{mod}\, q),\ s = (xr + kH(M))(\mathrm{mod}\, q),$$

$$\alpha = g^{-q(x(H(M)^{-1} - a_4 q - a_2) - a_3 H(M)^{-1} - kH(M) a_4 + a_3 a_4 q - a_1 - k a_4) \bmod p} \bmod q,$$

$$a_1 = [\, s\, \mathrm{H}^{-1}(M) / q], a_2 = [(q\text{-}r)\mathrm{H}^{-1}(M) / q], a_3 = [s / q],\ a_4 = [\, \mathrm{H}^{-1}(M) / q]$$

формулалар ёрдамида, имзони текшириш $u = \alpha (g^{u_1} y^{u_2} \mod p)(\mathrm{mod}\, q)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s, α) имзо коррект, лекин бардошсиз ҳисобланади.

Бу ерда, $y = g^x (\mathrm{mod}\, p)$, $u_1 = sw \bmod q$, $u_2 = (q - r)w \bmod q$, $w = H(M)^{(q-2)} \bmod q$ ва p, q, g - параметрлар ГОСТ Р 34.10-94 ЭРИ алгоритми каби генерация қилинади, H(M)-берилган M маълумот хэш қиймати.

Теорема 8. Агар k имзо эгасига маълум бирор $(0 < k < q)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = (g^k (\mathrm{mod}\, p))(\mathrm{mod}\, q),\ s = (xr + kH(M))(\mathrm{mod}\, q),$$

$$\alpha = -q(\, x(H^{-1}(M) - a_4 q - a_2) - a_3 H^{-1}(M) - kH(M) a_4 + a_3 a_4 q - a_1 - k a_4),$$

$$a_1 = [\, s\, \mathrm{H}^{-1}(M) / q], a_2 = [(q\text{-}r)\mathrm{H}^{-1}(M) / q], a_3 = [s / q],\ a_4 = [\, \mathrm{H}^{-1}(M) / q].$$

формулалар ёрдамида, имзони текшириш $u = g^{\alpha}(g^{u_1}y^{u_2} \bmod p)(\bmod q)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s, α) имзо коррект ва бардошли ҳисобланади.

Бу ерда, y, u_1 , u_2 , H(M) ва p, q, g – параметрлар теорема 7 каби аниқланган.

Диссертация иши **4.3-параграфида** мураккаб модул (факторизация ва дискрет логарифмлаш мураккаблиги) асосида бардошли электрон рақамли имзо алгоритмларини яратишнинг турли вариантлари ва улар криптотаҳлили босқичлари кўриб ўтилган.

Айтайлик, M – имзоланиши керак бўлган маълумот, $y=g^x \bmod N$, y-очиқ калит, x, $0<x<q$ оралиқдан олинган ёпиқ калит, $N=p_1 * q_1$ ҳамда p_1, q_1 ва q етарли катта туб сонлар бўлиб, $g^q \bmod N = 1$ ва $g^N \bmod N = 1$ шартлар бажарилсин. Бу ерда p_1, q_1 - ёпиқ параметрлар.

Теорема 9. Агар k имзо эгасига маълум бирор $(1< k < N)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = g^k \bmod N,\ s = (xr+kH(M)) (\bmod \varphi(N)),$$

формулалар ёрдамида, имзони текшириш $u = g^{u_1} y^{u_2} \bmod N$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект, лекин бардошсиз. Бу ерда $\varphi(N)$ - Эйлер функцияси, $u_1 = (s\ t) \bmod N$, $u_2 = (N-r)\ t \bmod N$, $t = H(M)^{-1} \bmod q$.

Теорема 10. Агар k имзо эгасига маълум бирор $(1< k < N)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = g^k \bmod N,\ s = (xr+kH(M))(\bmod N)$$

формулалар ёрдамида, имзони текшириш $u = g^{u_1} y^{u_2} \bmod N$ формула орқали амалга оширилса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект, лекин бардошсиз. Бу ерда, u_1 , u_2 қийматлар теорема 9 каби аниқланган.

Демак, кўриб чиқилган вариантдаги ЭРИ алгоритмлари бардошсиз экан. У ҳолда, мазкур алгоритмларга тегишли ($g^q \bmod N = 1$ ва $g^N \bmod N = 1$ шартлар бажарилмасин каби) ўзгартиришлар киритиш зарурати мавжуд.

Айтайлик, M – имзоланиши керак бўлган маълумот, $y=g^x \bmod N$, y - очиқ калит, x - ёпиқ калит, $N=p_1 * q_1$ ҳамда p_1, q_1, q - етарли катта туб сонлар ҳамда p_1, q_1 - имзо ёпиқ параметрлари бўлсин.

Теорема 11. Агар k имзо эгасига маълум бирор $(1< k < N)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = g^k \bmod N,\ s = (xr+kH(M))(\bmod \varphi(N)),\ a_1 = \left[\frac{s \cdot t}{N}\right],\ a_2 = \left[\frac{(N-r) \cdot t}{N}\right],$$

$$a_4 = \left[\frac{H(M) \cdot t}{q}\right],\ a_5 = \left[\frac{t}{q}\right],\ \alpha = g^{q(a_5 kH(M)+a_5 xN-a_4 k)+N(-tx+a_1+a_2 x)} \bmod N$$

формулалар ёрдамида, имзони текшириш $u = \alpha\, g^{u_1} y^{u_2} \bmod N$ формула орқали амалга оширилса, у ҳолда M маълумотга қўйилган (r, s, α) - имзо коррект, лекин бардошсиз. Бу ерда, u_1 , u_2 қийматлар теорема 9 каби аниқланган.

Демак, таклиф этилган учта вариантдаги мураккаб модулли ЭРИ алгоритмлари бардошсиз экан. Қуйида мазкур камчиликларни бартараф этиш масаласи кўриб чиқилган.

Теорема 12. Агар k имзо эгасига маълум бирор $(1< k < N)$ тасодифий сон, r, s ва α қийматлар қуйидаги:

$$r = g^k \bmod N,\ s = (xr+kH(M))(\bmod \varphi(N)),\ a_1 = \left[\frac{s\cdot t}{N}\right],\ a_2 = \left[\frac{(N-r)\cdot t}{N}\right],$$

$$a_4 = \left[\frac{H(M)\cdot t}{q}\right],\ a_5 = \left[\frac{t}{q}\right],$$

$$\alpha = (q(a_5 kH(M) + a_5 xN - a_4 k) + N(-tx + a_1 + a_2 x)) \bmod \varphi(N)$$

формулалар ёрдамида, имзони текшириш $u = g^{\alpha} g^{u_1} y^{u_2} \bmod N$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r,s,α) имзо коррект ва бардошли. Бу ерда, u_1, u_2 қийматлар теорема 9 каби аниқланган.

Диссертациянинг **«Эллиптик эгри чизиқ асосида бардошликлари оширилган электрон рақамли имзо алгоритмларини яратиш»** деб номланган бешинчи бобида эллиптик эгри чизиқда дискрет логарифмлаш мураккаблик масаласига асосланган янги ЭРИ алгоритмлари таклиф этилган ва улар криптотаҳлили жараёнлари келтирилган. ЭРИ алгоритмлари учун ишлаб чиқилган дастурий таъминот ёрдамида самарадорликлари баҳоланган.

Диссертация ишининг **5.1-параграфида** эллиптик эрги чизиқда дискрет логарифмлаш масаласига асосланган янги ЭРИ алгоритмлар таклиф этилган ва улар криптотаҳлили масалалари кўриб чиқилган. Шунингдек, мазкур мураккаблик асосида бардошсиз ЭРИ алгоритмлари бўйича тасдиқлар исбот қилинган.

Таклиф этилган эллиптик эгри чизиқ асосидаги янги ЭРИ алгоритмлари учун қуйидаги теоремалар ўринли.

Теорема 13. Айтайлик, имзони шакллантириш ва текширишда Q очиқ ва d ёпиқ $(0<d<n)$ калитлар орасидаги боғланиш $[d]G(x_1,y_1) = Q(x_2,y_2)$ бўлсин. Агар k имзо эгасига маълум бирор $(1 \le k \le n-1)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = ([k]G(\bmod n))_x,\ \ s := (k - dr)z \bmod n$$

формулалар, имзони текшириш $r := x(\bmod n)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект ва бардошли ҳисобланади.

Бу ерда x, эллиптик эгри чизиққа тегишли $X := [u]G + [r]Q = (x, y)$ нуқта абциссаси, $u = e \cdot s(\bmod n)$, $e := h(M \,||\, r)$, h – бардошли хэш алгоритм қиймати, M - имзоланиши керак бўлган маълумот, $z := e^{-1}(\bmod n)$, n – сони G базавий нуқта тартиби.

Теорема 14. Айтайлик, имзони шакллантириш ва текширишда Q очиқ ва d ёпиқ $(0 < d < n)$ калитлар орасидаги боғланиш $[d^{-1}]G(x_1,y_1) = Q(x_2,y_2)$ бўлсин. Агар k имзо эгасига маълум бирор $(1 \le k \le n-1)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = ([k]G(\bmod n))_x,\ \ s := (k - d^{-1}r)z \bmod n$$

формулалар, имзони текшириш $X := [u]G + [r]Q = (x, y)$, $r := x(\mathrm{mod} n)$ формула орқали амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r, s) имзо коррект ва бардошли ҳисобланади. Бу ерда, d^{-1} берилган d ёпиқ калит учун mod n бўйича тескари элемент.

Айтайлик, ЭРИ алгоритми Q очиқ ва d ёпиқ калитлар орасидаги боғланиш: $[d]G(x_1,y_1) = Q(x_2,y_2)$ мураккаблик асосида берилган бўлсин.

Теорема 15. Агар k имзо эгасига маълум бирор $(0 < k < n)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = ([k]G(\mathrm{mod} n))_x,\ s = (k - hd)r^{-1}(\mathrm{mod} n)$$

формулалар, имзони текшириш эса $r = [[rs]G + [h]Q]_x(\mathrm{mod} n)$ формула билан амалга оширилган бўлса, у ҳолда M маълумотга қўйилган (r,s) имзо коррект, лекин бардошсиз ҳисобланади.

Теорема 16. Агар k имзо эгасига маълум бирор $(0 < k < n)$ тасодифий сон, r ва s қийматлар қуйидаги:

$$r = ([k]G(\mathrm{mod} n))_x,\ s = (k - h)r^{-1}d^{-1}(\mathrm{mod} n);$$

формулалар, имзони текшириш $r = (([h]G + [rs]Q))_x(\mathrm{mod} n)$ формула орқали амалга оширилса, у ҳолда M маълумотга қўйилган (r,s) имзо коррект, лекин бардошсиз ҳисобланади.

Диссертация иши **5.2-параграфида** эллиптик эгри чизиқ асосидаги янги ЭРИ алгоритмлари ишлаб чиқилган дастурий таъминот ёрдамида самарадорликлари баҳоланган.

Мазкур жараёнда эллиптик эгри чизиқ параметрлари ГОСТ Р 34.10-2012 ЭРИ стандарт алгоритми назорат мисолидаги каби танланган ва узунликлари 77 ҳамда 154 байт бўлганда натижалар ўзаро солиштирилган.

Қуйида 7-жадвалда 154 байт маълумотни имзолаш ва текшириш учун сарфланган вақт натижалари келтирилган.

7-жадвал.

Имзолаш ва текшириш жараёнларига сарфланган вақтлар

Алгоритм номи	Очиқ ва ёпиқ калитлар	Имзолаш ва текшириш формулалари	Имзолашга кетган вақт	Имзони текширишга кетган вақт
1-ЭРИ алгоритм	$Q = [d]G$	$s := (k - dr)z \bmod n$ $X := [hs]G + [r]Q$	322(ms)	336(ms)
2-ЭРИ алгоритм	$Q = [d^{-1}]G$	$s := (k - d^{-1}r)z \bmod n$ $X := [hs]G + [r]Q$	328(ms)	340(ms)
ГОСТ Р 34.10-2012	$Q = [d]G$	$\mathrm{s} := (\mathrm{dr} + \mathrm{ke}) \bmod n$ $X := [h^{-1}s]G + [-rh^{-1}]Q$	331(ms)	339(ms)

ECDSA	$Q = [d]G$	$s := k^{-1}(e + dr) \bmod n$ $X := [s^{-1}h]G + [s^{-1}r]Q$	327(ms)	347(ms)

8-жадвалда умумий ҳолда турли узунликдаги ёпиқ калитларда алгоритмлар имзолаш жараёнларига сарфланган вақт кўрсатилган.

8-жадвал.

Турли узунликдаги ёпиқ калитлар ёрдамида имзолашга сарфланган вақт

Алгоритм номи	77 байт узунликдаги ёпиқ калит учун	154 байт узунликдаги ёпиқ калит учун	Вақтнинг ўзгариши (марта ортган)
1-ЭРИ алгоритм	272(ms)	322(ms)	1.184
2- ЭРИ алгоритм	322(ms)	328(ms)	1.019
ГОСТ Р 34.10-2012	272(ms)	331(ms)	1.217
ECDSA	259(ms)	327(ms)	1.263

Шунингдек, диссертация иши мазкур параграфида эллиптик эгри чизиқ асосидаги бардошли янги ЭРИ алгоритмларининг амалиётда қўлланиши нуқтаи назаридан катта разряддаги қийматларда тегишли назорат мисоллари келтирилган.

ХУЛОСА

«**Бардошли криптографик алгоритмлар яратиш усулларини ишлаб чиқиш**» мавзусидаги докторлик диссертацияси бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Блокли симметрик шифрлаш алгоритмларини умумий криптографик талабларга баҳолаш бўйича тавсиялар ишлаб чиқилган.

2. O‘z DSt 1105:2009 стандарти, ГОСТ Р 34.12-2015 стандарти Магма ва Кузнечик алгоритмлари S-блоклари умумий криптографик талабларга баҳоланган.

3. O‘zDSt 1105:2009 стандарт алгоритмида S-блок вазифасида келувчи *BaytAlmash* акслантириши учун чизиқсизлик қиймати юқори ва калитга боғлиқсиз янги математик формула таклиф этилган.

4. Маълумотни эллиптик эгри чизиқ нуқталари кўринишида ифодалаш усулидан фойдаланиб, эллиптик эгри чизиққа асосланган янги оптимал асимметрик шифрлаш алгоритми таклиф этилган.

5. Янги оптимал асимметрик шифрлаш алгоритми бардошлилиги актив криптотаҳлил усуллари билан баҳоланган.

6. Чекли майдонда дискрет логарифмлаш, эллиптик эгри чизиқда дискрет логарифмлаш мураккабликларига асосланган ва мураккаб модулли янги электрон рақамли имзо алгоритмлари таклиф этилган.

7. Турли мураккаблик асосида таклиф этилган янги электрон рақамли имзо алгоритмлари бардошлиги улар қадамларига тегишли криптоҳужум усулларини қўллаш билан исбот қилинган.

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

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

КУРЬЯЗОВ ДАВЛАТЁР МАТЯКУБОВИЧ

РАЗРАБОТКА СОЗДАНИЯ МЕТОДОВ СТОЙКИХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

05.01.07 – Методы и системы защиты информации. Информационная безопасность

АВТОРЕФЕРАТ
докторской (DSc) диссертации по физико-математическим наукам

ТАШКЕНТ – 2022

Тема докторской (DSc) диссертации по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за B2021.4.DSc/FM185.

Диссертация выполнена в Национальном университете Узбекистана имени Мирзо Улугбека.

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

Научный консультант:	**Арипов Мирсаид Мирсаидович** доктор физико-математических наук, профессор
Официальные оппоненты:	**Каримов Мадият Малиевич** доктор технических наук, профессор
	Жураев Гайрат Умарович доктор физико-математических наук, доцент
	Туйчиев Гулом Нумонович доктор физико-математических наук
Ведущая организация:	**Таджикский технический университет имени Ислама Каримова**

Защита диссертации состоится «11» июня 2022 года в 14[00] часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за №49). (Адрес: 100174, г.Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 246-02-24).

Автореферат диссертации разослан «30» мая 2022 года.
(протокол рассылки № 2 от 02.04.2022 года).

Р.Д. Алиев
Заместитель председателя Научного совета по присуждению научных степеней, д.ф.-м.н., профессор

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

Г.У. Жураев
Председатель научного семинара при Научном совете по присуждению научных степеней, д.ф.-м.н., доцент

ВВЕДЕНИЕ (аннотация докторской (DSc) диссертации)

Актуальность и востребованность диссертации. Исследования решений криптологических задач, ведущиеся в мире, проводятся в большинстве случаев по проблемам определения сеансового ключа алгоритмов симметричного шифрования, поиска закрытого ключа на основе открытого ключа асимметричных алгоритмов, определения коллизий хэш-функций и по проблемам разработки криптоатак на основе шагов алгоритма. Изучение свойств преобразования алгоритмов шифрования, разработка стойких алгоритмов асимметричного шифрования и электронной цифровой подписи на основе новых математических сложностей, являются объектом исследований в таких областях, как информационная безопасность, криптография, криптоанализ, прикладная математика и объектно-ориентированное программирование. Поэтому создание методы криптографической защиты информации, постоянный анализ стандартов и совершенствование криптостойкости алгоритмов остается одной из важных задач в области информационной безопасности.

В настоящее время в мире широко изучаются криптографические алгоритмы как наиболее надежные средства обеспечения безопасности информации, передаваемой по сети телекоммуникации.

Стандарты алгоритмов широко используются в криптомодулях программных, аппаратно-программных средств криптографической защиты информации. Поэтому оценка соответствия алгоритмов симметричного шифрования общим криптографическим требованиям, создание новых, различной сложности, стойких алгоритмов асимметричного шифрования и электронной цифровой подписи, а также разработка их программного обеспечения является одним из целевых научных исследований.

В нашей стране также уделяется большое внимание таким актуальным направлениям, как разработка стойких криптографических алгоритмов защиты информации, криптография и криптоанализ, которые являются научным и практическим применением фундаментальных наук. Значительные результаты были достигнуты в совершенствовании национальных стандартов и создании новых алгоритмов. Проведение научных исследований на уровне международных стандартов по приоритетным направлениям: «Алгебра и функциональный анализ, Прикладная математика и математическое моделирование, Вычислительная математика и дискретная математика, Теория вероятностей и математическая статистика»[3], были определены как основные задачи и направления деятелности.

Для обеспечения исполнения данного постановления важное значение обретает, разработка новых стойких симметричных, асимметричных алгоритмов шифрования и электронных цифровых подписей, оценка их стойкости и внедрение в практику полученных научных результатов.

[3] Постановление Президента Республики Узбекистан №ПП–4708 «О мерах по повышению качества образования и развитию научных исследований в области математики» от 07 мая 2020 года.

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

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

Обзор зарубежных научных исследований по теме диссертации[4].

Исследования по разработке симметричных и асимметричных алгоритмов и их стойкости проводятся ведущими мировыми высшими учебными заведениями и исследовательскими центрами, в том числе: National Institute of Standards and Technology - NIST, University of California, Conterpane Internet Security (США), University of Oxford (Великобритания), University of Haifa, Tel Aviv University, Weizmann Institute (Израил), Concordia Institute for Information Systems Engineering, Concordia University (Канада), Dian Ji University, Jiaotong University (Китай), Swiss Federal Institute of Technology (Швейцария), Vienna Technical University (Австрия), Nanyang Technological University (Сингапур), Al-Balqa Applied University, Yarmouk University (Иордания), Математическими институтами РАН РФ, Академии криптографии, Московским государственным университетом, Южным федеральным университетом, Московским государственным техническим университетом, Институтом криптографии, связи и информатики Федеральной службы безопасности Российской Федерации (ФСБ) (Россия),

[4] Обзор зарубежных научных исследований по теме диссертации составлен на основе следуюших источников: Journal of Cryptography and Communications, Journal of Cryptology, Journal of Mathematical Cryptology, Journal of Cryptographic Engineering, International journal of Applied Cryptography, Journal of Cryptologic Research, Журнал Математические вопросы криптографии.

Белорусским государственным университетом, Университетом информатики и радиоэлектроники, НИИ проблемы защиты информации (Беларусь), Институтом прикладной математики и механики АН Украины, Киевским политехническим институтом (Украина), Национальным университетом Казахстана, Институтом информационной безопасности и криптологии (Казахстан), Национальным университетом Узбекистана, Ташкентским университетом информационных технологий, ЦНТМИ ГУП “UNICON.UZ” (Узбекистан) которые проводят масштабные исследования.

В результате мировых исследований по разработке асимметричного шифрования, алгоритмов электронной цифровой подписи на основе различных математических сложностей, анализу стандарта алгоритма ГОСТ Р 34.12-2015 и разработке стойких S-блоков получен ряд научных результатов, в том числе следующие: разработаны асимметричные алгоритмы шифрования и электроно-цифровой подписи RSA (University of California, США) - основанной на задаче факторизации и EL-GAMAl (National Institute of Standards and Technology, США) – основанной на задаче дискретного логарифмирования в конечном поле; разаботан новый асимметричный алгоритм шифрования основанный на кодировании с помощью слов английского языка(Al-Balqa Applied University, Yarmouk University, Иордания), произведена оценка его стойкости; разаботаны и оценена стойкость новых алгоритмов электронно-цифровой подписи, коллективной подписи (Санкт-Петербургский государственный унверситет электротехники, Россия); доказана стойкость алгоритма Кузнечик стандарта ГОСТ Р 34.12-2015 после 3-го раунда к линейному и дифференциальному методам криптоанализа (Южный федеральный университет, Россия); оценена стойкость функции имитозащиты стандарта ГОСТ Р 34.12-2015 (Технический комитет в области защиты информации, Академия криптографии, Россия); разработан алгоритм представления данных в виде точки на эллиптической кривой и выражения точки эллиптической кривой в виде данных (Санкт-Петербургский институт информатики и автоматизации Академии наук, Россия); разработан асимметричный алгоритм шифрования на эллиптической кривой в конечном поле со специальной характеристикой (Санкт-Петербургский государственный технический университет), произведена оценка его стойкости; оценена стойкость стандартов алгоритмов электронно-цифровой подписи и протоколы основанные на сложности задачи дискретного логарифмирования на эллиптических кривых (Киевский политехнический институт, Харьковский университет радиоэлектроники, Украина); разработаны методы генерации S-блоков с высокой нелинейностью и степенью алгебраической нелинейности (Vienna Technical University, Katholieke Universite Leuven, Бельгия); разработаны методы генерации булевых функций с высокой нелинейностью (Indian Statistical Institute, Ҳиндистон, University of Science and Technology of China, Хитой, University of Alabama, АҚШ).

Научные исследования ведутся по ряду приоритетных направлений симметричных и асимметричных алгоритмов по всему миру, в том числе:

оценка преобразований алгоритмов симметричного шифрования; усовершенствование существующих сетей симметричного шифрования и разработка новых алгоритмов на их основе; разработка методов генерации стойких S-блоков для алгоритмов шифрования; оценка стойкости алгоритмов шифрования к современным методам криптоанализа; разработка методов генерации булевых функции с высокими значениями нелинейности; разработка новых постквантовых асимметричных алгоритмов, основанных на сложности решения задач в квантовых компьютерах; разработка нового стойкого асимметричного алгоритма шифрования на основе эллиптической кривой; разработка новых алгоритмов электронной цифровой подписи на основе задач дискретного логарифмирования в конечном поле, составного модуля и дискретного логарифмирования на эллиптической кривой, а также разработка их комплекса программных средств.

Степень изученности проблемы. На сегодняшний день для оценки стойкости алгоритмов симметричного шифрования существуют линейный, дифференциальный, линейно-дифференциальный, слайдовый, интегральный и алгебраический методы криптоанализа, теории которых разработаны М.Мацуи, Э.Бихам, А.Шамир, М.Хеллман, С.Лэнгфорд, А.Брюковым, Д.Вагнер, К.Шеннон, Н.Кортуа, А.Климовым, Ж.Патариным, Л.Кнудсен соответственно.

Проблемы оценки существующих алгоритмов симметричного шифрования современными методами криптоанализа изучались рядом ученых, в частности:

S-блоки алгоритма шифрования ГОСТ 28147-89 А.Е.Жуковым, Н.Молдовяном, А.Молдовяном по общим криптографическим требованиям, Л.Бабенко, Е.Ищуковой дифференциальным методом, Б.Абдурахимовым, А.Саттаровым линейно-дифференциальным и алгебраическим методами, Р.Алоевым, Б.Ахмедовым методом слайдовых атак; М.Ариповым, Г.Туйчиевым линейным и дифференциальным методами для симметричных алгоритмов шифрования на основе сети Лея-Месси; Е.Ищуковым, А.Марахимовым, Г.Джураевым стойкость алгоритма Кузнечик стандарта ГОСТ Р 34.12-2015 к дифференциальным и линейным методами, а также Б.Абдурахимовым, И.Бойкузиевым интегральным и алгебраическим методами; В.Гусевым оценка функции имитозащиты стандарта ГОСТ Р 34.13-2015; Б.Абдурахимовым и О.Аллановым методом интегрального и алгебраического анализа оценен стандарт алгоритма O‘zDSt1105:2009.

Кроме того П.Хасановым, М.Каримовым, Х.Хасановым разработан национальный блочный симметричный алгоритм шифрования на основе алгебры параметров.

Разработка асимметричных алгоритмов и оценка их криптостойкости рассмотрены в следующих научных работах: первый асимметричный алгоритм в криптографии - протокол генерации сеансового ключа симметричного алгоритма шифрования У.Диффи и М.Хэллманом; алгоритмы RSA и GAMAL Р.Райвеста, А.Шамира, Л.Адлемана и Т.Джамола; асимметричное шифрование и алгоритмы ЭЦП на основе алгебры

параметров М.Каримова, О.Ахмедовой, Назаровой М.Х.; алгоритмы ЭЦП и криптопротоколы основанные на задаче дискретного логарифмирования на эллиптической кривой Н.Молдовяна, А.Молдовяна, Б.Изотова, Э.Дерновой, Ю.Гурьянова, Manoj Kumar Chande, Chend-Chi Lee, Chun-Ta Li, Nissa Mehibel, M'hamed Hamadouche; алгоритмы электронной цифровой подписи основанные на задаче дискретного логарифмирования на эллиптической кривой в алгебре параметров, предложены в работах П.Хасанова, Х.Хасанова и О. Ахмедовой.

Генерация параметров эллиптических кривых (*a, b, p, G,* [n]G) по требованиям стойкости были исследованы в работах А.Ростовцева, Е.Маховенко, А.Буренкова, анализ стойкости алгоритмов электронной цифровой подписи на основе эллиптических кривых И.Горбенко, С.Збитнева, А.Полякова. Также проводились научные исследования по информационной безопасности и криптографии в нашей стране А.Кабуловым, С.Ганиевым, Р.Хамдамовым, К.Керимовым, Д.Иргашевой, Д.Акбаровым, З.Худайкуловым и другими учеными республики.

Связь темы диссертации с научно-исследовательскими работами высшего учебного заведения, в которых выполнялась диссертация.

Исследование диссертации выполнено в соответствии с планом НИР Национального университета Узбекистана «Алгоритмы и программное обеспечение для решения задач прикладной математики».

Целью исследования является разработка стойких алгоритмов симметричного, асимметричного шифрования и электронной цифровой подписи.

Задачи исследования состоят в следующем**:**

разработка рекомендаций по созданию алгоритмов симметричного шифрования повышенной стойкости;

оценка стандартов алгоритмов O‘zDSt 1105:2009 и ГОСТ Р 34.12-2015 на соответствие общим криптографическим требованиям;

разработка математических моделей алгоритмов асимметричного шифрования на основе эллиптических кривых повышенной стойкости;

разработка алгоритмов повышенной стойкости электронной цифровой подписи, основанных на сложности дискретного логарифмирования;

разработка алгоритмов электронной цифровой подписи повышенной стойкости на основе комбинированной сложности (с составным модулем - факторизация и дискретное логарифмирование в конечном поле);

разработка алгоритмов электронной цифровой подписи повышенной стойкости на основе сложности дискретного логарифмирования на эллиптической кривой.

Объект исследования - алгоритмы симметричного шифрования, методы криптоанализа, методы оценки алгоритмов общим криптографическим требованиям, алгоритмы асимметричного шифрование и электронной цифровой подписи.

Предмет исследования составляют этапы разработки стандартов алгоритмов шифрования, оценки стандартов алгоритмов O‘zDSt 1105:2009

и ГОСТ Р 34.12-2015 на общие криптографические требования. Разработка и оценка криптостойкости алгоритмов асимметричного шифрования на основе задачи сложности дискретного логарифмирования на эллиптической кривой и алгоритмов электронной цифровой подписи различной сложности.

Методы исследования. В диссертации использованы методы прикладной криптографии и криптоанализа, алгебры и теории чисел, дискретной математики, вычислительной математики, теории вероятностей и технологии объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

разработан метод оценки преобразования стандартов алгоритмов симметричного шифрования на соответствие требованиям сбалансированности, регулярности, нелинейности, коррелиационной иммунности, независимости выходящих битов;

доказано, значение нелинейности S-блоков стандарта ГОСТ Р34.12-2015 является высоким по стойкости, а S-блок стандарта O‘zDSt 1105: 2009 нестойким;

разработано нелинейное преобразование для стандарта алгоритма O‘zDSt 1105:2009 независящее от ключа и обеспечивающее высокие криптографические требования с использованием операций параметрической алгебры;

разработан новый алгоритм асимметричного шифрования на основе эллиптической кривой с использованием алгоритмов представления данных в виде точки на эллиптической кривой и выражения точки эллиптической кривой в виде данных;

разработан новый оптимальный асимметричный алгоритм шифрования на основе эллиптической кривой, который стойкий к методу активной атаки;

разработаны новые алгоритмы электронной цифровой подписи с повышенной стойкостью, основанные на сложности дискретного логарифмирования в конечном поле, дискретного логарифмирования на эллиптической кривой и составных модулей.

Практические результаты исследования состоят в следующем:

разработано программное обеспечение оценивающее алгоритмы симметричного шифрования общим криптографическим требованиям;

разработаны новые алгоритмы асимметричного шифрования на основе эллиптической кривой и их программное обеспечение;

доказана криптографическая стойкость новых алгоритмов электронной цифровой подписи, основанная на различных математических сложностях.

Достоверность результатов исследования.

Достоверность утверждений, полученных в диссертации, основана на строгости математических соображений, доказанных с использованием методов теории чисел, дискретной математики, криптографии и криптоанализа и сравнением результатов вычислительных экспериментов с набором созданных программ.

Научная и практическая значимость результатов исследования.

Научная значимость результатов исследования заключается в том, что предлагаемый метод проверки на соответствие общим криптографическим требованиям, алгоритмов асимметричного шифрования и электронной цифровой подписи может быть использован для обеспечения задачи конфиденциальности, аутентификаци информации передаваемой по сетям телекоммуникаций и безопасного обмена сеансовыми ключами алгоритма симметричного шифрования.

Практическая значимость результатов исследования заключается в том, что разработанные рекомендации могут быть использованы в качестве соответствующей методики приемки национальных стандартов алгоритмов, при подготовке экспертных заключений и проведении научно-исследовательских работ по разработке новых алгоритмов повышенной стойкости симметричного, асимметричного шифрования и электронной цифровой подписи, а также оценки теоретической и практической стойкости к методам криптоанализа.

Внедрение результатов исследований.

Полученные научные результаты в рамках исследовательской работы по разработке методов создания стойких криптографических алгоритмов внедрены в практику по следующим:

метод оценки требованиям сбалансированности, регулярности, нелинейности, коррелиационной иммунности, независимости выходящих битов стандартов симметричных алгоритмов, результаты оценки S-блоков стандартов алгоритмов O‘zDSt 1105:2009 и ГОСТ Р 34.12-2015, новый оптимальный асимметричный алгоритм основанный на сложности дискретного логарифмирования в эллиптической кривой были внедрены в крипто модулях программных и аппаратно-программных средств защиты информации, предназначенных для защиты обрабатываемой информации (справка Уполномоченного органа в области криптографической защиты информации, №20/5888 от 30 октября 2021 года). Применение научных результатов дало возможность генерации стойких S-блоков для симметричных алгоритмов шифрования, передачи сеансовых ключей алгоритма шифрования по незащищённому каналу связи, а также разработке надежного механизма защиты информации ограниченного доступа;

новые алгоритмы электронной цифровой подписи, основанные на сложности дискретного логарифмирования в конечном поле, дискретного логарифмирования на эллиптической кривой и составных модулей, которые были использованы при решение задачи аутентификации в проекте ЦНТМИ ГУП «UNICON.UZ» «Разработка методов и средств совершенствования услуг безопасности инфраструктуры открытых ключей Республики Узбекистан» (справка Министерства по развитию информационных технологий и коммуникаций №33-8/771 от 11 февраля 2022г.). Применение научных результатов позволило обеспечить безопасность инфраструктуры открытых ключей, а предложенная математический модель для стандарта алгоритма O‘zDSt 1105:2009 повысила его криптостойкость;

новый алгоритм оптимального асимметричного шифрования, методы и результаты оценки S-блоков стандартов алгоритмов O‘zDSt 1105:2009 и ГОСТ Р 34.12-2015 были использованы при защите данных информационных систем в рамках гранта №Ф706-17-«Исследование применения биометрико-криптографических технологий в информационных системах» (справка Министерства по развитию информационных технологий и коммуникаций №33-8/771 от 11 февраля 2022г.). Применение научных результатов позволило использовать асимметричные алгоритмы в схемах «шифрование-подпись» или «подпись-шифрование».

Апробация результатов исследования. Результаты данного исследования были обсуждены на 12 научно-практических конференциях, в том числе на 6 международных и 6 республиканских.

Публикация результатов исследования. По теме диссертации опубликована 31 научная работа, из них 19 входят в перечень научных изданий, предложенных Высшей аттестационной комиссией Республики Узбекистан для защиты докторских диссертаций, в свою очередь 5 из них опубликованы в зарубежных журналах и 14 в республиканских научных изданиях. 2 научные статьи внесены в международную базу данных Scopus. Получены 2 свидетельства о регистрации программных средств для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и 10 приложений. Объем диссертации составляет 184 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснованы актуальность и востребованность диссертации, описаны цели и задачи, объект и предмет исследования, соответствие приоритетным направлениям развития науки и технологий республики. Приведен обзор зарубежных научных исследований по теме диссертации и оценена степень изученности проблемы, сформулированы цели и задачи, выявлены объект и предмет исследования, изложены научная новизна и практические результаты исследования, раскрыты научные и практические значения полученных результатов, даны сведения о внедрении в практику результатов исследований, об опубликованных работах и о структуре диссертации.

В первой главе диссертации «**Оценка стандартов блочных симметричных алгоритмов на соответствие общим криптографическим требованиям**» приведены рекомендация по оценке стандартных алгоритмов симметричного шифрования на соответствие общим криптографическим требованиям, результаты проверки соответствия общим криптографическим требованиям преобразования стандарта алгоритма шифрования O‘zDSt 1105:2009 и S-блоков алгоритма Магма и Кузнечик ГОСТ Р 34.12-2015.

В параграфе 1.1 диссертации приводится описание понятий, необходимых для математической основы оценки соответствия стандартных алгоритмов симметричного шифрования общим криптографическим

требованиям, а также рекомендации по оценке соответствия преобразования вновь предложенного или существующего блочного симметричного стандартного алгоритма шифрования общим криптографическим требованиям.

В параграфе 1.2 диссертации дается оценка по общим криптографическим требованиям преобразования Qo‘shBosqichKalit, Sur, BaytAlmash стандарта алгоритма шифрования O‘zDSt 1105:2009 и на основе их результатов предлагается новая математическая модель для нелинейного преобразования BaytAlmash.

Результаты, полученные в этом разделе, представлены ниже в форме следующих утверждений.

Утверждение 1. Для преобразований Qo‘shBosqichKalit и Sur стандарта алгоритма O‘zDSt 1105:2009 общее значение нелинейности $N(\varphi)=0$.

Утверждение 2. В отношении примера, приведенного в приложении стандарта O'zDSt 1105:2009, преобразование *BaytAlmash* регулярно, значение нелинейности компонентов соответствующих булевых функций $N(f_1)=102$, $N(f_2)=106$, $N(f_3)=102$, $N(f_4)=102$, $N(f_5)=100$, $N(f_6)=106$, $N(f_7)=104$, $N(f_8)=98$, алгебраическая степень нелинейности равна 7, общее значение нелинейности равно 92 и степень корреляционной иммунности равна 0.

Согласно теории общих криптографических требований**,** максимальная степень алгебраической нелинейности сбалансированной функции **с** восьми аргументами должна быть равна 7, а общее значение нелинейности должено быть равно 112.

Таким образом, результаты проверки таблицы *S*-блоков по общим криптографическим требованиям преобразования *BaytAlmash,* приведенной в контрольном примере приложении стандарт O'zDSt 1105:2009, не в полной степени раскрывают криптографические свойства данного преобразования.

В данном преобразовании используя программное обеспечение, созданное в отношении значений тройных параметров (*D, R, L*)**,** при помощи преобразования *BaytAlmash* условно произведена генерация 10 различных таблиц *S*-блоков и были получены следующие результаты для общих значений нелинейности (Таблица 1):

Таблица 1

Значение общей нелинейности для различных десяти S-блоков

S-блоки	**D**	**R**	**L**	**Значение $N(\varphi)$**
BaytAlmash – 1	37	54	2	0
BaytAlmash – 2	31	8	2	15
BaytAlmash – 3	33	8	6	0
BaytAlmash – 4	119	198	2	14
BaytAlmash – 5	49	54	3	0

BaytAlmash – 6	65	160	2	0
BaytAlmash – 7	81	164	5	0
BaytAlmash – 8	93	168	7	3
BaytAlmash – 9	131	172	11	15
BaytAlmash – 10	121	246	4	0

Утверждение 3. В преобразовании *BaytAlmash* сгенерированных от неизвестного ключа для S-блоков 1, 3, 5, 6, 7, 10 общее значение нелинейности равно $N(\varphi)=0$, а для 2, 4, 8, 9 S-блоков общее значение нелинейности равно $N(\varphi)=15$, $N(\varphi)=14$, $N(\varphi)=3$ и $N(\varphi)=15$ соответственно.

Следовательно, в алгоритме O‘zDSt 1105:2009 для различных вариантов секретного ключа требуется внедрение генераторов, которые обеспечивают максимальное общее значение нелинейности (т.е. для сбалансированной булевой функции с 8 аргументами общее значение нелинейности равно 112).

Следующая математическая формула предлагается в качестве вводимого изменения на преобразование *BaytAlmash* стандарта O‘zDSt 1105:2009.

Утверждение 4. Если преобразование *BaytAlmash* алгоритма шифрования O‘zDSt 1105:2009 генерируется с использованием математической модели $BaytAlmash(x, z)=y$, $y=M\cdot(x\circledR z)^{-1}+v$, то общее значение нелинейности для данного преобразования равно $N(\varphi)=112$.

Здесь M, v – фиксированные матрицы и вектора, приведенные в преобразовании *SubBytes* стандарта AES, z – мастер ключ, $x, y, z \in GF(2^8)$, операция $^{-1}$ – обратный элемент в поле $GF(2^8)$, операция ® – умножение по параметру R многочленов 7-степени элементов в поле $GF(2^8)$ и исчисление остатка по многочлену 8-степени, неприводимому в этом поле (например: $x^8+x^6+x^5+x^3+1$).

В **параграфе 1.3** диссертации произведена оценка в соответствии с общими криптографическими требованиями S-блоков алгоритма Магма стандарта ГОСТ Р 34.12-2015.

Утверждение 5. Для S_i-блоков (i=1,…,8) алгоритма Магма преобразования регулярны, общие значения нелинейности равны 4, степень алгебраической иммунности равны 2, значение не связанности выходных битов (BIC) равны 0.

Утверждение 6. Значения нелинейности для всех компонентов булевых функций S_i-блоков (i=1,…,8) алгоритма Магма равны $N(f_1)=4$, $N(f_2)=4$, $N(f_3)=4$, $N(f_4)=4$, значение корреляционной иммунности всех булевых функций равно 0 и степень алгебраической нелинейности равно соответственно:
S_1, S_2, S_5, S_7: $deg\ (f_1) = 2$, $deg\ (f_2) = 3$, $deg\ (f_3) = 3$, $deg\ (f_4) = 3$.
S_3, S_4, S_6, S_8: $deg(f_1) = 3$, $deg\ (f_2) = 3$ $deg\ (f_3) = 3$, $deg\ (f_4) = 3$.

В **параграфе 1.4** диссертации произведена оценка соответствия общим криптографическим требованиям S-блоков алгоритма Кузнечик стандарта ГОСТ Р 34.12-2015.

Утверждение 7. Для S-блока алгоритма Кузнечик преобразование регулярное, общее значение нелинейности равно 100, степень алгебраической иммунности равна 3, а значение не связанности выходных битов равно 0.

Утверждение 8. Для компонентов булевых функций S-блока алгоритма Кузнечик значения нелинейности равны $N(f_1)=104$, $N(f_2)=106$, $N(f_3)=116$, $N(f_4)=104$, $N(f_5)=110$, $N(f_6)=106$, $N(f_7)=102$, $N(f_8)=104$ соответственно, значение корреляционной иммунности равно 0 и степень алгебраической нелинейности равно 7.

Сравнение значений, полученных при оценке S-блоков различных алгоритмов шифрования, с общими криптографическими требованиями, приведено в Таблице 2 ниже.

Таблица 2.

Сравнение результатов оценки S-блоков по общии криптографическим требованиям

Общие криптографические требования	**Магма**	**ГОСТ 28147-89**	**Кузнечик**	**AES**
	S-блоки $GF(2^4) \to GF(2^4)$	S-блоки $GF(2^4) \to F(2^4)$	S-блок $GF(2^8) \to GF(2^8)$	S-блок $GF(2^8) \to GF(2^8)$
Сбалансированность	+	+	+	+
Регулярность	+	+	+	+
deg(f)	2 или 3	3	7	7
$N(f)$	4	2 или 4	102-116	112
N(φ)	4	2	100	112
$CI(f)$	0	0	0	0
$AI(S)$	2	2	3	2
BIC(S)	0	0	0	0

Во второй главе диссертации **«Разработка нового алгоритма асимметричного шифрования на основе эллиптической кривой»** приведены математические основы современных алгоритмов асимметрич-ного шифрования, алгоритмы выражения данных в виде точек эллиптической кривой, математическая модель нового алгоритма шифрования на основе эллиптической кривой и полученные по ней результаты.

В параграфе 2.1 диссертации описываются математические основы задач, связанных с переносом асимметричных алгоритмов на эллиптические кривые.

В параграфе 2.2 диссертации описан алгоритм представления блоков данных в виде точек эллиптической кривой.

В процессе шифрования данных асимметричным алгоритмом на основе эллиптической кривой возникают следующие проблемы:

В частности, во время процесса шифрования значение данных M также должно быть точкой эллиптической кривой. Однако, на практике значение

данных не всегда выполняют данное условие. Поэтому для решения этой проблемы были предложены следующие подходы.

Подход 1. Символы, используемые для представления зашифрованных данных (код ASC II), отображаются в виде точек относительно выбранной эллиптической кривой.

Недостатком этого подхода является наличие таблицы, представляющей точки эллиптической кривой в соответствии с кодом ASC II, известным сторонам шифрования и дешифрования.

Подход 2. Шифруемая информация делится на соответствующие длины, и ее блоки отображаются с использованием соответствующего алгоритма в виде точек эллиптической кривой.

В диссертационной работе при разработке нового алгоритма асимметричного шифрования применен 2-й подход.

Ниже приведены алгоритмы для выражения m блоков данных, подлежащих шифрованию, в виде точки $M(x, y)$ эллиптической кривой и преобразования их в представление m данных.

Алгоритм отображения блоков данных в виде точек эллиптической кривой:

1. Счетчик устанавливается на i=0, вычисляется $p' = p\ div\ 2^{\pi-\mu}$, p' и m_i сравниваются как двоичные числа (div – это операция выделения целой части). Если $p' > m_i$, переходит к шагу 2, в противном случае переходит к шагу 3.

2. Если $i < 2^{\rho}$, то формируется строка r длиной ρ бит с двоичным значением, равным i и переходит к шагу 7. В противном случае появится сообщение «Точка эллиптической кривой не существует».

3. Если $i < 2^{\rho-1}$, то формируется строка r длиной $\rho - 1$ бит с двоичным значением, равным i и переходит к шагу 4. В противном случае появится сообщение «Точка эллиптической кривой не существует».

4. Переменной $\boldsymbol{x}$ присваивается значение $m_i||r$, вычисляется значение $w = (x^3 + ax + b)\mathrm{mod}\, p$.

5. Вычисляется значение символа Лежандра $\lambda = (\frac{w}{p})$. Если $\lambda = -1$, счетчик увеличивается на единицу $(i \leftarrow i + 1)$ и переходит на шаг 3, в противном случае переходит к шагу 6.

6. Вычисляется два значения $y_{1,2} = \pm\sqrt{w}\,(\mathrm{mod}p)$ корня, где $y_{1,2} \in \{1, 2, \dots, p - 1\}$, наименьшее значение $y_{1,2}$ присваивается к y и переходит к шагу 10.

7. Переменной x присваивается значение $m_i||r$ и вычисляется $w = (x^3 + ax + b)\mathrm{mod}\, p$ значение.

8. Вычисляется символ Лежандра $\lambda = (\frac{w}{p})$. Если $\lambda = -1$, то счетчик увеличивается на единицу $(i \leftarrow i + 1)$ и переходит на шаг 2, в противном случае он переходит на шаг 9.

9. Вычисляется два значения: $y_{1,2} = \pm\sqrt{w}\,(\mathrm{mod} p)$ корня, где $y_{1,2} \in \{1, 2, \dots, p-1\}$, большее из значений $y_{1,2}$ присваивается переменной y и переходит к шагу 10.

10. Результирующая пара координат (x, y) объявляется как точка $M(x, y)$, эллиптической кривой для соответствующего блока m.

Точка $M(x, y)$, выраженная точкой эллиптической кривой, преобразуется в представление данных с использованием следующего алгоритма.

1. Вычисляется $w = (x^3 + ax + b) \bmod p$.

2. Вычисляется $y_{1,2} = \pm\sqrt{w} \bmod p$ и проверяется условие $y_1 < y_2$, при этом $y_1, y_2 \in \{1,2, \dots, p-1\}$.

3. Если $y = y_1$, то берется значение $m = x\ div\ 2^{p-1}$, иначе берется значение $m = x\ div\ 2^p$.

В параграфе 2.3 диссертации приведена новая математическая модель алгоритма асимметричного шифрования на основе эллиптической кривой, с использованием алгоритмов выражения m блоков данных в виде точек $M(x, y)$, принадлежащих эллиптической кривой и преобразования точки эллиптической кривой в виде m блоков данных.

Для определения асимметричного алгоритма необходимо описать основные математические объекты, используемые в процессе шифрования и преобразования данных в исходный текст. Ниже приведены основные математические определения и требования к объектам асимметричного алгоритма.

Предположим, что алгоритм асимметричного шифрования использует эллиптическую кривую, определяемую формулой $y^2 \equiv x^3 + ax + b \pmod{p}$, и следующие параметры:

a) простое число p – модуль эллиптической кривой, удовлетворяющее неравенство $p > 2^{255}$. Верхняя граница данного числа определяется при конкретной реализации схемы асимметричного алгоритма;

b) эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;

d) простое число n – это порядок циклической подгруппы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} w = l * n, l \in Z, l \geq 1 \\ 2^{254} < n < 2^{256} \end{cases}$$

e) $G(x_0, y_0)$ – базовая точка с координатами (x_0, y_0) эллиптической кривой E, удовлетворяющая равенство $[n]G = 0$ и $G \neq 0$;

К параметрам алгоритма асимметричного шифрования предъявляются следующие требования:

a) Для всех целых чисел $i = 1, 2 \dots, B$ должно выполняться условие $p^i \neq 1 \pmod{n}$, где для B выполняется неравенство $B \geq 31$;

b) должно выполняться неравенство $w \neq r$;

d) инвариант $J(E) \neq 0$ кривой должен удовлетворять условию $J(E) \neq 0$ или 1728.

Каждый пользователь алгоритма асимметричного шифрования должен обладать следующими личными ключами:

а) d закрытый ключ асимметричного алгоритма, целого числа удовлетворяющий неравенство $0<d<n$;

d) $Q(x, y)$ открытый ключ асимметричного алгоритма, является точкой эллиптической кривой, удовлетворяющей равенство $[d]G=Q$.

Математическая модель предлагаемого алгоритма асимметричного шифрования состоит из следующей последовательности шагов.

m сообщение, подлежащих шифрованию, при условия $\rho = \pi - \mu = 16$ делятся на μ битовые блоки ($m = \{m_1, m_2, \dots, m_i\}$, $|m_i| = \mu$ бит, где разряд простого числа p равен π бит).

I. Процесс шифрования данных.

1. Выбирает число k из диапазона $0 < k < n$ и это число известно только сторонешифрующей данные.

2. Вычисляется $C_1 = [k]G$, $R = [k]Q$ точки эллиптической кривой.

3. Проверяется, является ли шифруемая блок информация точкой эллиптической кривой. Если данные не являются точкой эллиптической кривой переходит к шагу 7, в противном случае выполняются следующие вычисления.

4. Вычисляется значение y_1, y_2 по абсциссе x зашифрованной точки $M(x, y)$. Если $y = \min(y_1, y_2)$, переходит к шагу 6, в противном случае выполняются следующие вычисления.

5. Вычисляется $C_2 = M + R$ точка эллиптической кривой и для значения $q = 3$ выполняется $t = x_{C_2} || q$ и переходит к шагу 8 (здесь $|q| \to 2$ бит).

6. Вычисляется $C_2 = M + R$ точка эллиптической кривой и для значения $q = 1$ выполняется $t = x_{C_2} || q$ и переходит к шагу 8 (здесь $|q| \to 2$ бит).

7. Вычисляется $C_2 = M \cdot R = (x_{C_2}, y_{C_2})$ (или формула $x_{C_2} = m_i \oplus x_R$) и выполняется $t = x_{C_2} || q$, где $\mathrm{q} = 0$ и переходит к шагу 8 (здесь $|q| \to 2$ бит).

8. $C = \{C_1, t\}$ объявляется зашифрованный текст.

II. Процесс преобразования зашифрованного текста в открытый текст.

1. Вычисляется $U(x_u, y_u) = [d]C_1$.

2. Если выполняется условие q=0, переходит к шагу 8, в противном случае к шагу 3.

3. Если q=3 то переходит к шагу 4, если q=1, то переходит к шагу 6.

4. Вычисляется $w = x_{C_2}^3 + a x_{C_2} + b \pmod p$.

5.Вычисляется $y_{1,2} = \pm\sqrt{w} \pmod p$ и выбирается $y = \max(y_1, y_2)$, переходит к шагу 9.

6. Вычисляется $w = x_{C_2}^3 + a x_{C_2} + b \pmod p$.

7. Вычисляется $y_{1,2} = \pm\sqrt{w} \pmod p$ и выбирается $y = \min(y_1, y_2)$ и переходит к шагу 9.

8. Из формулы $M = \frac{x_{C_2}}{x_U}$ вычисляется открытый текст.

9. Точка эллиптической кривой $M(x,y)$ вычисляется формулой $M = (x_{C_2}, y) - U(x_u, y_u)$.

10. Точка $M(x,y)$ с использованием алгоритма выражения в виде данных m переводится в форму блока открытого текста.

Для предложенного алгоритма асимметричного шифрования доказана следующая теорема.

Теорема 1. Алгоритм асимметричного шифрования на основе эллиптической кривой, который включает 8 шагов для шифрования данных и 10 шагов для преобразования зашифрованного текста в открытый текст, является корректным.

В параграфе пункте 2.4 диссертации представлен анализ результатов, полученных с помощью нового алгоритма асимметричного шифрования, основанного на эллиптической кривой.

В таблице 3 приводятся результаты для объема памяти, занимаемого данными в предлагаемом алгоритме асимметричного шифрования на основе эллиптической кривой.

Таблица 3.

Полученные результаты по объему

Длина сообщений (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Представление в виде точки (байт)	1 276 766	6 429 202	12 841 346	128 510 799
Процесс шифрования (байт)	1 275 581	6 378 273	12 757 262	127 572 670
Процесс расшифрования (байт)	1 276 766	6 429 202	12 841 346	128 510 799
Восстановление сообщений (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Измененный объем шифр текста (%)	21,65 % увеличилось	21,66 % увеличилось	21,66 % увеличилось	21,66 % увеличилось

В таблице 4 приводится время, необходимое для шифрования и преобразования в открытый текст данных в алгоритме асимметричного шифрования на основе эллиптической кривой.

Таблица 4.

Затраченное время для процесса шифрования и расшифрование

Длина сообщений (байт)	1 048 576	5 242 880	10 485 760	104 857 600
Затраченное время для представления блоков данных в виде точек на эллиптической кривой (секунд)	20	100	199	1998
Затраченное время для процесса шифрования (секунд)	122	612	1223	12235
Затраченное время для процесса расшифрования (секунд)	118	591	1179	11807
Затраченное время для восстановления сообщения (секунд)	5	25	50	499
Общее затраченное время (минут)	$4\frac{5}{12}$ мин	$22\frac{2}{15}$ мин	$44\frac{11}{60}$ мин	$442\frac{19}{60}$ мин

Разработано соответствующее программное обеспечение для сравнения результатов, полученных с помощью алгоритма асимметричного шифрования, на основе эллиптической кривой, со стандартными алгоритмами асимметричного шифрования RSA и Эль-Гамаля. На основании полученных результатов имеет место следующее утверждение.

Утверждение 9. Предложенный алгоритм шифрования на основе эллиптической кривой занимает в памяти место на 16,65% больше, чем алгоритм RSA и в 2,2 раза быстрее по скорости.

Утверждение 10. Предлагаемый алгоритм шифрования на основе эллиптических кривых занимает на 78,35% меньше памяти, чем алгоритм Эль-Гамаля, и в 4,65 раза быстрее по скорости.

В третьей главе диссертации **«Разработка алгоритма асимметричного шифрования с повышенной стойкостью на основе эллиптической кривой»,** изложены вопросы, связанные с применением активной криптоатаки к современным алгоритмам асимметричного шифрования, математической моделью нового оптимального алгоритма асимметричного шифрования, стойкого к активной криптографической атаке.

В параграфе 3.1 диссертации излагаются вопросы, связанные с применением метода активной крипто-атаки к современным алгоритмам асимметричного шифрования.

Определение. Действия как прерывание процесса передачи конфиденциальных данных, модификация, подготовка поддельных зашифрованных данных, называются активной атакой.

В настоящее время в современной асимметричной криптографии, исходя из активной криптоатаки: “Атака на основании выбранного открытого текста (chosen-plaintext attack-CPA)”, “Атака на основании выбранного шифрованного текста (chosen-ciphertext attack-CCA)”,“Атака на основании адаптивно выбранного шифрованного текста (adaptive chosen-ciphrtext attack-CCA2)”, разработаны основные требования для стойкости асимметричных криптосистем.

Исходя из требований к стойкости асимметричных криптосистем имеет место следующее утверждение.

Утверждение 11. Стандартный алгоритм RSA нестойкий к активному криптографическому методу атаки.

В целом данное утверждение справедливо не только к стандарту алгоритма RSA, но и ко всем алгоритмам асимметричного шифрования. В частности, алгоритм асимметричного шифрования основанный на задаче сложности дискретного логарифмирования на эллиптической кривой, предложенный в главе 2 диссертации, считается нестойким к активным методам криптоатак.

В результате возникает необходимость в разработке оптимальной версии данного алгоритма.

В **параграфе 3.2** диссертации разработана математическая модель нового оптимального алгоритма асимметричного шифрования.

Сегодня на практике стандартный алгоритм RSA используется как алгоритм RSA-OEP, с добавлением схемы заполнения, приведенной в классической литературе.

Эта ситуация приводит к необходимости совершенствования алгоритма асимметричного шифрования, основанного на эллиптической кривой, предложенного в главе 2. Ниже приводится оптимальный алгоритм асимметричного шифрования для шифрования данных с использованием эллиптической кривой для этапов преобразования в открытый текст.

Алгоритм процесса шифрования.

Сторона шифрующая исходные данные *M*, случайным образом выбирает только известное число *k* - из диапазона 0 < *k* < *n*. Используя его, рассчитываются $C_1 = [k]G$ и $R = [k]Q$ - точки эллиптической кривой.

Заданные *M*-сообщения по условию $\mu = \pi - k_0 - k_1 - 16$ разбиваются на ($M = \{m_1, m_2, ..., m_v\}$, $|m_i| = \mu$ бит) битовые блоки.

Каждый $|m_i| = \mu$ блок открытого текста из битов длины заполняется k_0 нулями и шифруется отдельно в следующей последовательности.

1. Генерируются случайные *l* - данные длиной $k_1 = 128$ бит.
2. Вычисляется $S_1 = (m_i \| 0^{k_0}) \oplus Hesh1(l)$.
3. Вычисляется $S_2 = l \oplus Hesh2(S_1)$.
4. Генерируется информация $S = S_1 \| S_2$.

5. Проверяется условие, что S – информация является точкой $M\ (x, y)$ эллиптической кривой. Если данные не являются точкой эллиптической кривой, переходит к шагу 11.
6. С использованием x - координаты точки $M\ (x, y)$ вычисляется $w = \left(x^3 + ax + b\right) \bmod p$.
7. Вычисляются значения $y_{1,2} = \pm\sqrt{w} \left(\bmod p\right)$.
8. Если $y = \min(y_1, y_2)$, переходит к шагу 10.
9. Переменной q присваивается значение 3 (q = 3) и вычисляется $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \| q$ и переходит к шагу 12 (здесь $|q|$=2 бит).
10. Переменной q присваивается значение 1 (q = 1) и вычисляется $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \| q$ и переходит к шагу 12.
11. Переменной q присваивается значение 0 (q = 0) и вычисляется $x_{C_2} = S \oplus x_R$ $t = x_{C_2} \| q$.
12. $E_i = \{ C_1(x, y), t \}$ – объявляется как блок зашифрованного текста.

Преобразование зашифрованных блоков данных E_i (E_i={$C_1(x,y),t$}) в исходный текст.

1. Вычисляется точка эллиптической кривой $U\left(x_u, y_u\right) = [d]C_1$.
2. Если q = 0, то рассчитывается $S = x_{C_2} \oplus x_U$ и переходит к шагу 10.
3. Вычисляется $w = \left(x_{C_2}^3 + ax_{C_2} + b\right) \bmod p$.
4. Вычисляется $y_{1,2} = \pm\sqrt{w} \left(\bmod p\right)$.
5. Если q = 3, переходит к шагу 7.
6. Вычисляется $y=\min(y_1,y_2)$ и переходит к шагу 8.
7. Вычисляется $y=\max(y_1,y_2)$.
8. Вычисляется точка эллиптической кривой $M(x, y) = \left(x_{C_2}, y\right) - U\left(x_U, y_U\right)$.
9. Точка $M\ (x, y)$ представляется в виде S - данных .
10. Первый бит $\mu + k_0$ информации S загружается в S_1, последний бит k_1 в S_2 (т.е.: $C_2 C_1 \| S_2 = S$).
11. Вычисляется $l = S_2 \oplus Hesh2\left(S_1\right)$.
12. Вычисляется $Sm = S_1 \oplus Hesh1\left(l\right)$.
13. Если значение последнего k_0 – бита информации Sm равно нулю, то «данные достоверны», и первые μ – бит информации Sm объявляются в виде блока открытого текста, в противном случае как «ложная информация» (или фальшивая).

Здесь число μ определяет длину данных m_i в битах, p - простое число, p>3, π - символ, определяющий разряд заданного простого числа p; k_0, k_1 - натуральные числа, длины хэш-значений $Hesh1$ и $Hesh2$ соответственно являются устойчивыми хэш-функциями $\mu + k_0$ и k_1 бит.

Для предложенного нового оптимального алгоритма асимметричного шифрования доказано следующее.

Теорема 2. Оптимальный асимметричный алгоритм шифрования, основанный на эллиптической кривой, который включает в себя 12 шагов для шифрования данных, и 13 шагов для преобразования шифра в открытый текст, корректен и устойчив к активному способу криптоатаки.

В пункте 3.3 диссертации описан анализ результатов, полученных при использовании оптимального алгоритма асимметричного шифрования на основе эллиптической кривой.

Результаты оценки оптимального алгоритма асимметричного шифрования на основе эллиптической кривой с точки зрения объема памяти и параметров затраченного времени представлены в таблицах 5 и 6.

Таблица 5.

Объем занимаемой памяти для различных значений

Длина сообщения (байт)	37982	75964	151928	1 671 208
Заполнение сообщения (байт)	93504	187008	374016	4113792
Представление в виде точки (байт)	113671	227307	454671	5 001 086
Процесс шифрования (байт)	113756	227547	455026	5005191
Процесс расшифрования (байт)	113671	227307	454671	5 001 086
Восстановление сообщения из вида точки (байт)	93504	187008	374016	4113792
Восстановление сообщения (байт)	37982	75964	151928	1 671 208
Изменение объема шифртекста (%)	199 %	199 %	199 %	199 %

Таблица 6.

Затраченное время, для различных длин сообщение

Длина сообщений (байт)	37982	75964	151928	1 671 208
Затраченное время для заполнения сообщения (секунд)	0,639	1,294	2,589	27,728
Затраченное время для представления точки (секунд)	1,778	3,588	7,208	77,782
Затраченное время для процесса шифрования (секунд)	10,281	20,561	41,06	451,433
Затраченное время для процесса рашифрования (секунд)	10,281	21,092	41,356	451,83

Затраченное время для восстановления сообщения из точки (секунд)	0,421	0,827	1,654	18,665
Восстановление сообщение используя схему заполнения	0,624	1,263	2,48	27,22
Общее затраченное время (секунд)	24,413	48,625	96,347	1054,037

С использованием разработанного программного обеспечения результаты оптимального асимметричного алгоритма шифрования на основе эллиптической кривой сравнивались с результатами оптимального алгоритма шифрования RSA. Исходя из полученных результатов, имеют место следующие утверждения.

Утверждение 12. Оптимальный алгоритм RSA занимает на 150,79% больше памяти, чем алгоритм RSA, и работает в 2,4 раза медленнее по времени.

Утверждение 13. Оптимальный алгоритм шифрования, основанный на эллиптической кривой, занимает на 177,35% больше памяти, чем алгоритм шифрования на основе ЭЭЧ, и работает в 2,5 раза медленнее по скорости.

Утверждение 14. Предлагаемый оптимальный алгоритм шифрования, основанный на эллиптической кривой, занимает на 40% больше памяти, чем оптимальный алгоритм шифрования RSA, но по скорости работает в 2,4 раза быстрее.

В четвертой главе диссертации **«Разработка алгоритмов электронной цифровой подписи повышенной стойкости на основе дискретного логарифмирования и составного модуля»,** приведены методы фальсификации алгоритмов ЭЦП, предложены новые алгоритмы ЭЦП основанные на задаче дискретного логарифмирования в конечном поле, новые алгоритмы ЭЦП основанные на задачах сложности составных модулей (факторизация и дискретное логарифмирование) и представлены процессы их криптоанализа.

На сегодняшний день по результатам анализа создания современных алгоритмов ЭЦП выделяют три метода их поделки (фалсификации):

-путем эффективного решения математической сложности, использованной в подписи;

- путем коллизии хеш-значения;

- путем использования допущенных в алгоритме подписи ошибок.

В параграфе 4.1 диссертации на основе методов фальсификации алгоритмов ЭЦП описаны полученные результаты слабых алгоритмов ЭЦП, основанных на сложности дискретного логарифмирования.

Предположим, что при формировании и проверке подписи связь между x закрытыми и y открытыми ключами задана сложностью дискретной логарифмической задачи в конечном поле $y = g^x \bmod p$. В этом случае, согласно анализу алгоритмов ЭЦП доказано следующее.

Теорема 3. Если k является случайным числом $(0 < k < p)$, известным владельцу подписи, значения r и s исчислены следующими:

$$r = (g^k \bmod p),\ s = (k - hx)r^{-1} \pmod{p-1}$$

формулами, проверка подписи выполнена по формуле $r = y^h g^{rs} \pmod p$, то подпись (r, s), в сообщение M, является корректной, но слабой.

Теорема 4. Если k является случайным числом $(0 < k < p)$, известным владельцу подписи, значения r и s исчислены следующими:

$$r = g^k \pmod p,\ s = (k-h)r^{-1}x^{-1} \pmod{p-1}$$

формулами, проверка подписи выполнена по формуле $r = g^h y^{rs} \pmod p$, то подпись (r, s), в сообщение M, является корректной, но слабой.

В параграфе 4.2 диссертации приведены вопросы разработки новых алгоритмов ЭЦП на основе задачи дискретного логарифмирования в конечном поле и их криптоанализа.

Теорема 5. Если k является случайным числом $(0 < k < p)$, известным владельцу подписи, значения r, s, α исчислены следующими:

$r = (g^k \pmod p) \pmod q$, $s = k^{-1}(xr + H(M)) \pmod q$, $a_1 = [H(M)\, s^{-1} / q]$, $a_2 = [r\, s^{-1} / q]$, $a_3 = [s^{-1} / q]$, $\alpha \equiv g^{q(a_3(H(M)+xr)+a_1+a_2 x)} \bmod p \bmod q$ формулами, проверка подписи осуществлена по формуле: $u = \alpha\ (g^{u_1} y^{u_2} \bmod p) \pmod q$, то подпись (r, s, α), в сообщение M, является корректной, но слабой.

Здесь, $y = g^x \pmod p$, $u_1 = (H(M)\ w) \bmod q$, $u_2 = (r\ w) \bmod q$, $w = s^{-1} \bmod q$ и p, q, g – параметры генерируются как в алгоритме DSA ЭЦП, H(M)- хеш-значение, вычисленное из заданных M данных.

Теорема 6. Если k является случайным числом $(0 < k < p)$, известным владельцу подписи, значения r, s, α исчислены следующими:

$$r = (g^k \pmod p) \pmod q,\ s = k^{-1}(xr + H(M)) \pmod q,\ a_1 = [H(M)\, s^{-1} / q]$$

$$\alpha = q(a_3(H(M) + xr) + a_1 + a_2 x),\ ,\ a_2 = [r\, s^{-1} / q],\ a_3 = [s^{-1} / q]$$

формулами, проверка подписи осуществлена по формуле $u = g^{\alpha}(g^{u_1} y^{u_2} \bmod p) \pmod q$ то подпись (r, s, α), в сообщение M, является корректной и стойкой.

Здесь, y, u_1, u_2, $H(M)$ и p, q, g – параметры идентичны как в теореме 5.

Теорема 7. Если k является случайным числом $(1 \le k \le q)$, известным владельцу подписи, значения r, s, α исчислены следующими:

$$r = (g^k \pmod p) \pmod q,\ s = (xr + kH(M)) \pmod q,$$

$$\alpha = g^{-q(x(H(M)^{-1} - a_4 q - a_2) - a_3 H(M)^{-1} - kH(M) a_4 + a_3 a_4 q - a_1 - k a_4)} \bmod p \bmod q,$$

$$a_1 = [s\, H^{-1}(M) / q],\ a_2 = [(q-r) H^{-1}(M) / q],\ a_3 = [s / q],\ a_4 = [H^{-1}(M) / q],$$

формулами, проверка подписи осуществлена по формуле:

$u = \alpha\ (g^{u_1} y^{u_2} \bmod p) \pmod q$, то подпись (r, s, α), в сообщение M, является корректной, но слабой.

Здесь, $y = g^x \pmod p$, $u_1 = sw \bmod q$, $u_2 = (q-r)w \bmod q$, $w = H(M)^{(q-2)} \bmod q$ и p, q, g – параметры генерируются как в алгоритме ГОСТ Р 34.10-94 ЭЦП, H(M) - хеш значение, вычисленное из заданных M данных.

Теорема 8. Если k является случайным числом $(1 \le k \le q)$, известным владельцу подписи, значения r, s, α исчислены следующими:

$$r = (g^k \pmod p) \pmod q, \quad s = (xr + kH(M)) \pmod q,$$

$$\alpha = -q(x(H^{-1}(M) - a_4 q - a_2) - a_3 H^{-1}(M) - kH(M)a_4 + a_3 a_4 q - a_1 - ka_4),$$

$$a_1 = [s\,H^{-1}(M)/q],\ a_2 = [(q-r)H^{-1}(M)/q],\ a_3 = [s/q],\ a_4 = [H^{-1}(M)/q]$$

формулам, проверка подписи осуществляется по формуле $u = g^{\alpha}(g^{u_1} y^{u_2} \bmod p) \pmod q$, то подпись (r, s, α), в сообщение M, является корректной и стойкой.

Здесь, y, u_1, u_2, $H(M)$ и p, q, g – параметры идентичны как в теореме 7.

В параграфе 4.3 диссертации рассмотрены различные варианты создания стойких алгоритмов ЭЦП с составными модулями и этапами их криптоанализа.

Предположим, что M - данные, которые следует подписать, $y = g^x \bmod N$, y - открытый ключ, x секретный ключ из диапазона $0 < x < q$, $N = p_1 * q_1$ и p_1, q_1 и q - достаточно большие простые числа и выполнены условия $g^q \bmod N = 1$, $g^N \bmod N = 1$. Здесь p_1, q_1 – закрытые параметры.

Теорема 9. Если k является случайным числом $(1 < k < N)$, известным владельцу подписи, значения r, s исчислены следующими:

$$r = g^k \bmod N,\ s = (xr + kH(M)) \pmod{\varphi(N)},$$

формулами, проверка подписи выполнена по формуле $u = g^{u_1} y^{u_2} \bmod N$, то подпись (r, s), в сообщение M, является корректной, но слабой.

Здесь, $\varphi(N)$ - функция Эйлера, $u_1 = (s\ t) \bmod N$, $u_2 = (N-r)\ t \bmod N$, $t = H(M)^{-1} \bmod q$.

Теорема 10. Если k является случайным числом $(1 < k < N)$, известным владельцу подписи, значения r, s исчислены следующими:

$$r = g^k \bmod N,\ s = (xr + kH(M)) \pmod N$$

формулами, проверка подписи выполнена по формуле $u = g^{u_1} y^{u_2} \bmod N$, то подпись (r, s), в сообщение M, является корректной, но слабой.

Здесь, значение u_1, u_2 идентичены как в теореме 9.

Следовательно, алгоритмы ЭЦП в рассмотренном варианте нестойкие. В данном случае необходимо внести изменения в эти алгоритмы (не выполнение условий $g^q \bmod N = 1$ и $g^N \bmod N = 1$).

Предположим, что M - данные, которые следует подписать, $y = g^x \bmod N$, y - открытый ключ, x - закрытый ключ, $N = p_1 * q_1$ и p_1, q_1 и q - достаточно большие простые числа, p_1, q_1 – закрытые параметры подписи.

Теорема 11. Если k является случайным числом $(1 < k < N)$, известным владельцу подписи, значения r, s, α исчислены следующими:

$$r = g^k \bmod N,\ s = (xr + kH(M)) \pmod{\varphi(N)},\ a_1 = \left[\frac{s \cdot t}{N}\right],\ a_2 = \left[\frac{(N-r) \cdot t}{N}\right],$$

$$a_4 = \left[\frac{H(M) \cdot t}{q}\right],\ a_5 = \left[\frac{t}{q}\right],\ \alpha = g^{q(a_5 kH(M) + a_5 xN - a_4 k) + N(-tx + a_1 + a_2 x)} \bmod N$$

формулами, проверка подписи производится по формуле $u = \alpha\, g^{u_1} y^{u_2} \bmod N$, то подпись *(r, s),* помещенная в сообщение *M,* является корректной, но слабой. Здесь, значение u_1 , u_2 идентичены как в теореме 9.

Таким образом, алгоритмы ЭЦП составными модулями в трех предложенных вариантах являются нестойкими. Вопрос устранения этого недостатка обсуждается ниже.

Теорема 12. Если *k* является случайным числом (1< *k* < *N),* известным владельцу подписи, значения *r, s,* α исчислены следующими:

$$r = g^k \bmod N,\ s = (xr + kH(M))(\bmod \varphi(N)),\ a_1 = \left[\frac{s \cdot t}{N}\right],\ a_2 = \left[\frac{(N-r)\cdot t}{N}\right],$$

$$a_4 = \left[\frac{H(M)\cdot t}{q}\right],\ a_5 = \left[\frac{t}{q}\right],$$

$$\alpha = (q(a_5 kH(M) + a_5 xN - a_4 k) + N(-tx + a_1 + a_2 x)) \bmod \varphi(N)$$

формулами, проверка подписи производится по формуле: $u = g^{\alpha} g^{u_1} y^{u_2}$ *mod N,* то подпись *(r, s,* α *),* в сообщение *M,* является корректной и стойкой. Здесь, значение u_1 , u_2 идентичены как в теореме 9.

В пятой главе диссертации **«Разработка алгоритмов электронной цифровой подписи с повышенной стойкости на основе эллиптических кривых»,** предложены новые алгоритмы ЭЦП основанные на задачах сложности дискретного логарифмирования эллиптических кривых и процессы их криптоанализа, а также произведена оценка разработанных алгоритмов ЭЦП при помощи программного обеспечения.

В пункте 5.1 диссертации предлагаются математические модели новых алгоритмов ЭЦП, основанных на задаче дискретного логарифмирования эллиптической кривой и рассмотрены проблемы их криптоанализа.

Для предложенных новых алгоритмов ЭЦП, основанных на эллиптической кривой имеют место следующие теоремы.

Теорема 13. Предположим, что в формировании и верификации подписи, отношения между *Q* открытым и *d* (0 < *d* < n) закрытым ключами выражается как $[d]G(x_1,y_1) = Q(x_2,y_2)$. Если *k* является случайным числом $(1 \le k \le n-1)$, известным владельцу подписи, значения *r, s* исчислены следующими: $r = \left([k]G(\bmod n)\right)_x$, $s \coloneqq (k - dr)z \bmod n$ формулами, проверка подписи производится по формуле $r \coloneqq x(\bmod n)$, то подпись *(r, s),* в данные *M,* является корректной и стойкой. Здесь *x* является абсциссой точки эллиптической кривой $X \coloneqq [u]G + [r]Q = (x, y)$, $u = e \cdot s(\bmod n)$, $e \coloneqq h(M \parallel r)$, *h* – значение стойкого хэш-алгоритма, *M* сообщения, которые должны быть подписаны, число $z \coloneqq e^{-1}(\bmod n)$, *n* - порядок базовой точки *G*.

Теорема 14. Предположим, что отношение между *Q* открытыми и *d* закрытыми (0<d<n) ключами при формировании и проверке подписи выражается как $[d^{-1}]G(x_1,y_1) = Q(x_2,y_2)$. Если *k* является случайным числом $(1 \le k \le n-1)$, известным владельцу подписи, значения *r, s* исчислены следующими: $r = \left([k]G(\bmod n)\right)_x$, $s \coloneqq (k - d^{-1}r)z \bmod n$ формулами, проверка подписи производится по формуле $r \coloneqq x(\bmod n)$, то подпись *(r, s),*

в сообщение *M,* является корректной и стойкой. Здесь d^{-1} – элемент, обратный по mod *n* для данного закрытого ключа *d.*

Предположим, что соотношение между открытым *Q* и закрытым *d* ключами задано на основе сложности $[d]G(x_1,y_1) = Q(x_2,y_2)$.

Теорема 15. Если *k* является случайным числом *(0 < k < n),* известным владельцу подписи, значения *r, s* исчислены следующими:

$r = \left([k]G(\bmod n)\right)_x$, $s = (k - hd)r^{-1}(\bmod n)$ формулами, проверка подписи производится по формуле $r = \left[[rs]G + [h]Q\right]_x(\bmod n)$, то подпись *(r, s),* в сообщение *M,* является корректной, но слабой.

Теорема 16. Если *k* является случайным числом *(0 < k < n),* известным владельцу подписи, значения *r, s* исчислены следующими:

$r = \left([k]G(\bmod n)\right)_x$, $s = (k - h)r^{-1}d^{-1}(\bmod n)$ формулами, проверка подписи производится по формуле $r = (([h]G + [rs]Q))_x(\bmod n)$, то подпись *(r,s),* в сообщение *M,* является корректной, но слабой.

В параграфе 5.2 диссертации оценивается эффективность с использованием программного обеспечения, разработанного для новых алгоритмов ЭЦП на основе эллиптических кривых.

В этом процессе параметры эллиптической кривой выбраны, как в контрольном примере стандартного алгоритма ЭЦП ГОСТ Р 34.10-2012, и результаты взаимно сравнивались при длинах в 77 и 154 байта.

В таблице 7 показаны результаты времени затраченного на подписание и проверку 154 байтов данных.

Таблица 7.

Время, затраченное на процессы генерации и проверку подписи

Название алгоритма	Открытый и закрытый ключи	Формулы генерации и проверки подписи	Време для генерации подписи	Време для проверки подписи
1-алгоритм	$Q = [d]G$	$s := (k - dr)z \bmod n$ $X := [hs]G + [r]Q$	322(ms)	336(ms)
2-алгоритм	$Q = [d^{-1}]G$	$s := (k - d^{-1}r)z \bmod n$ $X := [hs]G + [r]Q$	328(ms)	340(ms)
ГОСТ Р 34.10-2012	$Q = [d]G$	$s := (dr + ke) \bmod n$ $X := [h^{-1}s]G + [-rh^{-1}]Q$	331(ms)	339(ms)
ECDSA	$Q = [d]G$	$s := k^{-1}(e + dr) \bmod n$ $X := [s^{-1}h]G + [s^{-1}r]Q$	327(ms)	347(ms)

В таблице 8 показано время, затраченное на процессы подписи алгоритма закрытыми ключами разной длины.

Таблица 8.

Время, затраченное на генерацию подписи для различной длины закрытого ключа

Название алгоритма	Для закрытого ключа длиной 77 байт	Для закрытого ключа длиной 154 байт	Изменение времени (повысилось в раз)
1-алгоритм	272(ms)	322(ms)	1.184
2-алгоритм	322(ms)	328(ms)	1.019
ГОСТ Р 34.10-2012	272(ms)	331(ms)	1.217
ECDSA	259(ms)	327(ms)	1.263

Также, в этом параграфе диссертации с точки зрения практического применения новых алгоритмов ЭЦП, основанных на эллиптических кривых, приведены контрольные примеры при больших значениях разрядов.

ЗАКЛЮЧЕНИЕ

В результате исследований, проведенных по докторской диссертации на тему **«Разработка методов создания стойких криптографических алгоритмов»** представлено следующее:

1. Разработаны рекомендации по оценке алгоритмов блочного симметричного шифрования на соответствие общим криптографическим требованиям.
2. Произведена оценка на соответствие общим криптографическим требованиям S-блоков стандартов O‘z DSt 1105:2009 и ГОСТ Р 34.12-2015, алгоритмов Магма и Кузнечик.
3. В стандартном алгоритме O‘z DSt 1105:2009 предложена новая математическая модель с высоким значением нелинейности и независимой от ключа функцией для преобразования *BaytAlmash,* которая представлена в виде функции S-блока.
4. Предложен новый оптимальный алгоритм асимметричного шифрования на основе эллиптической кривой, использующий метод выражения данных в виде точек на эллиптической кривой.
5. Методами активного криптоанализа оценена стойкость нового оптимального алгоритма асимметричного шифрования.
6. Предложены новые алгоритмы электронной цифровой подписи, основанные на сложности дискретного логарифмирования в конечном поле, дискретного логарифмирования в эллиптической кривой и с составными модулями.
7. Стойкость новых алгоритмов ЭЦП, предложенных на основе различной сложности, доказана путем применения разнообразных криптоатак.

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

NATIONAL UNIVERSITY OF UZBEKISTAN

KURYAZOV DAVLATYOR MATYAKUBOVICH

DEVELOPMENT OF METHODS FOR CREATING STRONG CRYPTOGRAPHIC ALGORITHMS

05.01.05 – Methods and systems of information protection. Information security

CONTENT OF DISSERTATION ABSTRACT OF THE DOCTOR OF PHYSICAL AND MATHEMATICAL SCIENCES (DSc)

TASHKENT – 2022

The subject of the doctor of sciences dissertation is registered by the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan B2021.4.DSc/FM185.

Dissertation has been prepared at the National University of Uzbekistan.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (summary)) on the website http://fti-kengash.uz/ and an the website of "ZiyoNet" Information and educational portal http://www.ziyonet.uz/.

Scientific consultant:	**Aripov Mirsaid Mirsidikovich** Doctor of physical and mathematical sciences, professor
Official opponents:	**Madjit Malikovich Karimov** Doctor of technical sciences, professor
	Gayrat Umarovich Jurayev Doctor of physical and mathematical sciences, dotsent
	Gulom Numonovich Tuychiev Doctor of physical and mathematical sciences
Leading organization:	**Tashkent State Technikal University named after Islam Karimov**

Defense will take place on "11" June 2022 at 14^{00} at the meeting of Scientific council number DSc.03/30.12.2019.FM.01.02 at the National University of Uzbekistan (Address: 100174, Uzbekistan, Tashkent city, Almazar area, University str. 4, Ph.: (99871) 227-12-24, fax: (99871) 246-53-21, 246-02-24, e-mail: nauka@nuu.uz).

The dissertation is possible to review in Information-resource centre at the National University of Uzbekistan (registered № 49) (Address: 100174, Uzbekistan, Tashkent city, Almazar area, University str., 4. Ph.: (99871) 246-02-24).

Abstract of dissertation sent out on "30" May 2022.
(mailing report № 2 on 02.05.2022).

R.D.Aloev
Deputy chairman of Scientific Council on award of scientific degrees, D.F.M.S., professor

Z.R. Rakhmonov
Scientific Secretary of Scientific Council on award of scientific degrees, D.F.M.S.

G.U.Jurayev
Chairman of Scientific Seminar under Scientific Council on award of scientific degrees, D.F.M.S., dotsent

INTRODUCTION (Doctor of Science's Thesis Annotation (DSc)

The aim of the research is to develop strong algorithms for symmetric, asymmetric encryption and electronic digital signature.

Research tasks include:

development of recommendations for the creation of high-strength symmetric encryption algorithms;

assessment of algorithms standards O'zDSt 1105:2009 and GOST R 34.12-2015 for compliance with general cryptographic requirements;

development of mathematical models of asymmetric encryption algorithms based on elliptic curves of increased strength;

development of algorithms for increased security of electronic digital signatures based on the complexity of factorization and discrete logarithm;

development of algorithms for electronic digital signatures of increased security on the basis of combined (with a composite module - factorization and discrete logarithm in a finite field) complexity;

development of algorithms for electronic digital signatures of increased security based on the complexity of discrete logarithm on an elliptic curve.

The object of the research is factorization, discrete logarithm in a finite field, questions of the complexity of discrete logarithm in an elliptic curve, symmetric encryption algorithms, cryptanalysis methods, assessment methods for general cryptographic requirements, asymmetric encryption and electronic digital signature algorithms.

Scientific novelty of the research work:

a method for evaluating the transformation of standard symmetric encryption algorithms for compliance with the requirements of balance, regularity, nonlinearity, correlation immunity, and independence of output bits has been developed;

proved that the value of the nonlinearity of the S-blocks of the GOST R 34.12-2015 standard is high in stability, and the S-block of the O'zDSt 1105:2009 standard is unstable

a nonlinear transformation has been developed for the O'zDSt 1105:2009 algorithm standard, independent of the key and providing high cryptographic requirements using parametric algebra operations

developed a new asymmetric encryption algorithm based on an elliptic curve using data presentation algorithms as a point on an elliptic curve and expressing an elliptic curve point as data;

a new optimal asymmetric encryption algorithm based on an elliptic curve has been developed, which is resistant to the method of active attack;

new algorithms for electronic digital signature of increased security have been developed, based on the complexity of discrete logarithm in a finite field, discrete logarithm on an elliptic curve and composite modules.

Implementation of the research results:

The obtained scientific results within the framework of research work on the development of methods for creating strong cryptographic algorithms are implemented in the following:

a method for evaluating the requirements of balance, regularity, nonlinearity, correlation immunity, independence of the output bits of symmetric algorithms standards, the results of the evaluation of S-blocks of the standards of algorithms O‘zDSt 1105:2009 and GOST R 34.12-2015, a new optimal asymmetric algorithm based on the complexity of discrete logarithm in an elliptic curve were implemented in the crypto modules of software and hardware and software means of information protection, designed to protect the processed information (reference №20/5888 of 30 October 2021 of the Authorized body in the field of cryptographic information protection). The application of scientific results made it possible to generate strong S-boxes for symmetric encryption algorithms, transfer encryption algorithm session keys over an unprotected communication channel, and also develop a reliable mechanism for protecting limited access information.

developed new electronic digital signature algorithms based on the complexity of discrete logarithm in a finite field, discrete logarithm on an elliptic curve and composite modules that were used to solve the authentication problem in State Unitary Enterprise (SUE) “UNICON.UZ” within the framework of the project “Improvement of methods and security tools for public key infrastructure services of the Republic of Uzbekistan” to solve authentication issues (reference №33-8/771 of 11 February 2022 of Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). The application of scientific results made it possible to ensure the security of the public key infrastructure, and the proposed mathematical model for the O‘zDSt 1105:2009 algorithm standard increased its cryptographic strength.

new algorithm for optimal asymmetric encryption, methods and results of evaluating the S-blocks of the O‘zDSt 1105:2009 and GOST R 34.12-2015 algorithm standards were used in data protection within the framework of the grant No. Ф706-17 “Research on the application of biometric-cryptographic technologies in information systems” (reference №33-8/771 of 11 February 2022 of Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan). The application of scientific results made it possible to use asymmetric algorithms in “encryption-signature” or “signature-encryption” schemes.

The structure and volume of the thesis. The dissertation consists of an introduction, five chapters, a conclusion, a bibliography and 10 appendices. The total volume of the dissertation is 184 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (I часть; I part)

1. Арипов М.М., Курьязов Д.М. Об одном алгоритме ЭЦП с составным модулем // Доклады Академии наук Республики Узбекистан, №4, 2012, 22-24. (01.00.00, №7).
2. Курьязов Д.М. Алгоритм ЭЦП на эллиптических кривых // Вестник Национального университета Узбекистана, №2, 2013, 87-90. (01.00.00, №8)
3. Курьязов Д.М. DSA ЭРИ алгоритми модификациялари ва уларнинг криптотахлили // Вестник Ташкентского университета информационных технологий, №2, 2012, 19-23. (05.00.00, №10).
4. Курьязов Д.М. ГОСТ Р34.10-94 ЭРИ алгоритми модификациялари ва уларнинг криптотахлили // Журнал проблемы информатики и энергетики, №4-5, 2012, 75-80. (05.00.00, №5).
5. Курьязов Д.М. Асимметричный алгоритм шифрование данных на эллиптической кривой // Вестник Ташкентского университета информационных технологий, №2, 2014, 56-62. (05.00.00, №10).
6. Курьязов Д.М. Миллий стандарт шифрлаш алгоритмига криптотаҳлил усулларини қўллаш билан боғлиқ масалалар // Журнал проблемы информатики и энергетики, №5, 2014, 95-100. (05.00.00, №5).
7. Курьязов Д.М. Губка схемасига асосланган маълумот аутентификация коди алгоритми. // Вестник Ташкентского университета информационных технологий, №4, 2015, 127-131. (05.00.00, №10).
8. Арипов М.М., Курьязов Д.М. Протокол слепой подписи, основанный на сложности решения двух трудных задач // Доклады Академии наук Республики Узбекистан, №6, 2015, 46-48. (01.00.00, №7).
9. Курьязов Д.М.Генерация совместного ключа методом эллиптических кривых // Журнал проблемы информатики и энергетики, №4, 2016, 101-107. (05.00.00, №5).
10. Курьязов Д.М. Губка схемасига асосланган узлуксиз шифрлаш алгоритми // Журнал Ахборот коммуникациялар: Тармоқлар, Технологиялар, Ечимлар, №4, 2015, 11-15. (05.00.00, №2).
11. Aripov M., Kuryazov D.M. Algorithm of without key hash-function based on Sponge-scheme // International Journal of Advances in Computer Science and Technology, 7(6), 2018, 40-42. (5. Global Impact Factor. IF=0,499).
12. Курьязов Д.М. Маълумот махфийлигини эллиптик эгри чизиқлар билан таъминлаш масалалари // Журнал Ахборот коммуникациялар: Тармоқлар, Технологиялар, Ечимлар, №3, 2018, 41-45. (05.00.00, №2).
13. Курьязов Д.М. SHA оиласига мансуб хэш функциялар тасодифийлигини NIST тестлари билан баҳолаш // Журнал проблемы информатики и энергетики, №2, 2018, 89-94. (05.00.00, №5).

14. Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves // International Journal of Advanced Trends in Computer Science and Engineering, 9(1), 2020, 295-298. (5. Global Impact Factor. IF=0,378).

15. Kuryazov D.M. Development of electronic digital signature algorithms with compound modules and their cryptanalysis // Journal of Discrete Mathematical Sciences and Cryptography, 24(4), 2021, 1085-1099. (3. Scopus. IF = 0,637).

16. Kuryazov D.M. Optimal asymmetric data encryption algorithm // Global Journal of Computer Science and Technology, 21(2), 2021, 29-33. (23. Scientific journal Impact factor. IF=8,286).

17. Курьязов Д.М. Эллиптик эгри чизиқ асосидаги электрон рақамли имзо алгоритмлари ва уларни қалбакилаштириш усуллари // Журнал Ахборот коммуникациялар: Тармоқлар, Технологиялар, Ечимлар, №2, 2021, 42-45. (05.00.00, №2).

18. Курьязов Д.М. Алгоритм электронно цифровой подпись основанные на сложности решения задач дискретного логарифмирования и факторизации // Бьюллетень института Математики, № 6, 2021, 82-85. (01.00.00 №17).

19. Aripov M., Kuryazov D.M. New algorithms for electronic digital elliptic curves // International Journal of Applied Mathematics & Information Sciences, 16(1), 2022, 121-125. (3, Scopus, IF=0.23).

II бўлим (II часть; II part)

20. Курьязов Д.М. Шифрлаш алгоритмлари криптобардошлигини баҳолаш усуллари ва улар билан боғлиқ айрим масалалар // Материалы научно-практической конференции «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения» (12 октября 2011г. УЗАСИ).-Ташкент, 2011.- с.19-21.

21. Курьязов Д.М. ЭЦП на эллиптических кривых с увеличенной стойкостью //Сборник докладов Республиканской научно-технической конференции молодых ученных, исследователей, магистрантов Информационные технологии и проблемы телекоммуникации» (14-15 марта 2013г. ТУИТ). -Ташкент. 2013.Часть 1. - с.254-255.

22. Арипов М.М., Курьязов Д.М. Анализ стойкости S – блока стандарта алгоритма O‘zDSt 1105:2009 // Сборник материалах I-Международной научно-практической конференций (12-13 сентября 2013г., Астана.).- Астана. 2013. -с. 109-116.

23. Курьязов Д.М. «Шифрлаш алгоритмларини лойихалаш босқичлари» //Сборник материалов Республиканской научно-технической конференции «Прикладная математика и информационная безопасность» (28-30 апреля 2014г. НУУз).-Ташкент. - с. 345-350.

24. Курьязов Д.М. Шифрлаш алгоритмлари математик асослари ва ривожланиш истиқболлари. //Сборник материалов Республиканской научно-технической конференции «Давлат жамият бошқарувида замонавий ахборот

технологияларини жорий этишнинг долзарб муаммолари» (17-18 апреля 2015г. АГУ). -Ташкент. 2015. -с.152-154.

25. Арипов М.М., Курьязов Д.М. Об одной алгоритм ЭЦП с увеличенной стойкости //Сборник материалах III-Международной научно-практической конференции (15-16 октября 2015г., Астана). - Астана. 2015. -с. 35-39.

26. Курьязов Д.М. Замонавий хэш алгоритмларини лойиҳалаш босқичлари //Сборник тезисов и докладов Республиканский семинар: «Информационная безопасность сфере связи и информатизации. Проблемы и пути их решения» (28 октября 2015г. Ташкент). –Ташкент. 2015. - с. 31-35.

27. Курьязов Д.М. Асимметрик алгоритмларни амалиётда қўллаш билан боғлиқ муаммолар ва улар ечимлари // Сборник в материалах международной научной конференции «Современные проблемы математики и физики» (6-10 октября 2017 г. НУУз).- Ташкент. 2017. -с. 186-188.

28. Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves // Transactions of the international scientific conference “Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2018” (13-15 September, 2018, Tashkent).- Tashkent. 2018. - pp.60.

29. Курьзов Д.М. Электрон рақамли имзо алгоритми ва уни қалбакилаштиришга қаратилган криптоҳужум усули // “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” мавзусидаги Республика илмий-техник семинар материаллари (29 октябрь 2020 йил, «UNICON.UZ» ДУК – Фан-техника ва маркетинг тадқиқотлари маркази). -Тошкент. 2020. -119-124 бет.

30. Kuryazov D.M. Assessment for general cryptographic requirements of S-block of the Magma algorithm // Transactions of the international scientific conference “Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2021”(November 15-17,2021).-Fergana.2021.-pp.208.

31. Kuryazov D.M. Assessment for general cryptographic requirements of S-block of the Kuznechik algorithm // Transactions of the international scientific conference “Contemporary mathematics and its application” (November 17-19, 2021). – Tashkent. 2021. – pp.92.

32. Курьязов Д.М. Электрон рақамли имзо. Электрон ҳисоблаш машинаси учун дастур. 09.07.2021й., №DGU 20211929, Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Интеллектуал мулк агентлиги.

33. Курьязов Д.М., Саттаров А.Б. Асимметрик шифрлаш алгоритми. Электрон ҳисоблаш машинаси учун дастур. 09.07.2021й., №DGU 20211928, Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Интеллектуал мулк агентлиги.

Автореферат «Ўзбекистон математика журнали» таҳририятида таҳрирдан ўтказилди.

Бичими 60x84 1/16. Ризограф босма усули. Times гарнитураси.

Шартли босма табоғи: 4,25. Адади 100. Буюртма № 24.
Баҳоси келишилган ҳолда.

«ЎзР Фанлар Академияси Асосий кутубхонаси» босмахонасида чоп этилган.
Босмахона манзили: 100170, Тошкент ш., Зиёлилар кўчаси, 13-уй.