MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/2025.27.12.FM.01.03 RAQAMLI ILMIY KENGASH

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI

BOYQUZIYEV ILXOM MARDANOQULOVICH

SIMMETRIK VA OCHIQ KALITLI SHIFRLASH ALGORITMLARINI BAHOLASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot va kiberxavfsizlik

FIZIKA-MATEMATIKA FANLARI DOKTORI (DSC) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2026

UDK: 004.056.55

Fizika-matematika fanlari doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

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

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

Boyquziyev Ilxom Mardanoqulovich
Simmetrik va ochiq kalitli shifrlash algoritmlarini baholash usullari va algoritmlari.....3

Бойкузиев Илхом Марданокулович
Методы и алгоритмы оценки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом.....29

Boykuziev Ilkhom Mardanakulovich
Methods and algorithms for evaluating symmetric and public key encryption algorithms 57

E'lon qilingan ishlar ro'yxati
Список опубликованных работ
List of published works.....62

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/2025.27.12.FM.01.03 RAQAMLI ILMIY KENGASH

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETI

BOYQUZIYEV ILXOM MARDANOQULOVICH

SIMMETRIK VA OCHIQ KALITLI SHIFRLASH ALGORITMLARINI BAHOLASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot va kiberxavfsizlik

FIZIKA-MATEMATIKA FANLARI DOKTORI (DSC) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2026

Fan doktori (DSc) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2026.DSc/FM316 raqam bilan ro‘yxatga olingan.

Dissertatsiya Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume) Ilmiy kengash web-sahifasida (www.nuu.uz) hamda “ZiyoNet” Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Abduraximov Baxtiyor Fayziyevich** fizika-matematika fanlari doktori, professor
Rasmiy opponentlar:	**Kuryazov Davlatyor Matyakubovich** fizika-matematika fanlari doktori
	Tuychiyev G‘ulom Numonovich fizika-matematika fanlari doktori
	Botirov Fayzullajon Baxtiyorovich texnika fanlari doktori, dotsent
Yetakchi tashkilot:	**O‘zbekiston Respublikasi Mudofa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti**

Dissertatsiya himoyasi Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti huzuridagi ilmiy darajalar beruvchi DSc.03/2025.27.12.FM.01.03 raqamli Ilmiy kengashning 2026-yil «__» _____ soat ____ dagi majlisida bo‘lib o‘tadi. (Manzil: 100174, Toshkent shahri, Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (99871) 227-12-24, faks: (99871) 246-53-21, e-mail: nauka@nuu.uz).

Dissertatsiya bilan Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti Axborot-resurs markazida tanishish mumkin (____ raqami bilan ro‘yxatga olingan).
Manzil: 100174, Toshkent shahri, Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (99871) 246-02-24

Dissertatsiya avtoreferati 2026-yil «____» _____ da tarqatildi.
(2026-yil «____» _____ dagi ____-raqamli reyestr bayonnomasi).

M.M. Aripov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, fizika-matematika fanlari doktori, professor

Z.R. Raxmonov
Ilmiy darajalar beruvchi Ilmiy kengash ilmiy kotibi, fizika-matematika fanlari doktori, dotsent

A.V. Kabulov
Ilmiy darajalar beruvchi Ilmiy kengash qoshidagi Ilmiy seminar raisi, texnika fanlari doktori, professor

KIRISH (fan doktori (DSc) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zaruriyati. Bugungi kunda jahon miqiyosida simmetrik va ochiq kalitli shifrlash algoritmlarini kriptotahlil usullariga baholash masalalariga oid tadqiqotlar dolzarb va zarur hisoblanadi, jumladan, chiziqsiz akslantirishlarning kriptotahlil usullariga bardoshliligini baholash, ochiq kalitli shifrlash algoritmlaridan faktorlash muammosiga asoslangangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitlarini aniqlash, shuningdek, ochiq kalitli shifrlash algoritmining yetarlicha katta modulini faktorlashga qaratilgan usul va algoritmlarni ishlab chiqish masalalariga alohida ahamiyat berilmoqda. Amaldagi kriptografik tizimlarda algoritmlar, qo‘llanilayotgan kalit uzunliklari va parametrlar zamonaviy kriptotahlil usullariga va hisoblash qurilmalari quvvatlariga nisbatan qayta baholab borilishi lozim. Chainalysis ma’lumotlariga ko‘ra, “2024-yilda dunyo bo‘yicha kriptografik tizimlarga qaratilgan hujumlar oqibatida yetkazilgan zarar 2023-yilga nisbatan 21.07% ga oshgan va 2.2 milliard AQSh dollarni tashkil qilgan” [1]. Bunday ko‘lamdagi zararlarning oldini olish uchun, kriptotizimlar xavfsizligini ko‘p darajali, kompleks yondashuv asosida, jumladan, matematik hisoblashlar murakkabligiga tayangan baholash usullari bilan baholab borish zarur. Shu nuqtai nazardan, simmetrik va ochiq kalitli shifrlash algoritmlarini baholash uchun zamonaviy kriptotahlil usullarini yaratish muhim vazifalardan biri bo‘lib qolmoqda.

Jahonda axborot xavfsizligini ta’minlash maqsadida bardoshli kriptografik algoritmlarni yaratish va ularning kriptobardoshligini oshirishga qaratilgan keng ko‘lamli ilmiy-tadqiqot ishlari olib borilmoqda. Bu borada, avvalo, kriptotahlil usullari yordamida amaldagi shifrlash algoritmlarining zaif tomonlarini aniqlash, ularni turli hujum modellariga nisbatan baholash hamda natijalar asosida xavfsiz va bardoshli algoritmlarni loyihalashga dolzarb vazifa sifatida qaralmoqda. Simmetrik shifrlash algoritmlarida qo‘llaniladigan chiziqsiz akslantirishlarning kriptobardoshliligini matematik mezonlar asosida baholash muhim ahamiyat kasb etadi. Differensial, chiziqli, algebraik kabi kriptotahlil usullarga bardoshlilikni ta’minlash maqsadida S-blok va boshqa chiziqsiz komponentlarning xossalarini tahlil qilishga, ochiq kalitli kriptografiyada esa tadqiqotlar shifrlash tizimlarining matematik asoslarini chuqur o‘rganish, ularning murakkablik darajasini baholash hamda mavjud va ehtimoliy hujumlarga nisbatan xavfsizligini ta’minlashga xizmat qiladigan yangi yondashuvlarga asoslangan baholash usullarini ishlab chiqishga alohida e’tibor berilmoqda.

Respublikamizda axborot xavfsizligini ta’minlash, xususan, kriptologiya sohasiga, axborotni kriptografik himoyasini tashkil etish, bardoshli kriptografik algoritmlarni va zamonaviy kriptotahlil usullarini yaratishga katta e’tibor qaratib kelinmoqda. Jumladan, so‘nggi yillarda kriptologiya sohasini ta’lim va ilm-fanni rivojlantirish bo‘yicha olib borilayotgan islohotlarda muayyan natijalarga erishilmoqda. O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293 sonli Qarorida axborotni

[1] https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

himoyalashda qo‘llanadigan kriptografik algoritmlarni doimiy ravishda takomillashtirib borishni taqozo etishi ta’kidlangan va ushbu Qaror bilan tasdiqlangan O‘zbekiston Respublikasida milliy kriptologiya sohasini rivojlantirishning dolzarb yo‘nalishlari bo‘yicha 2024 - 2028-yillarga mo‘ljallangan ilmiy-tadqiqot ishlari dasturida zamonaviy kriptotahlil usullarini yaratish bo‘yicha ilmiy-tadqiqot ishi bajarilishi ko‘zda tutilgan[2]. Ushbu vazifalarni amalga oshirishda zamonaviy kriptografik algoritmlarning kriptobardoshliligini baholash va tahlil qilishning yangi usullarini yaratish, yaratilgan usullar orqali kriptografik algoritmlarni baholash murakkabliklari bo‘yicha tajriba-sinovlarini o‘tkazish, ularning samaradorligini baholash muhim ahamiyat kasb etmoqda.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60 sonli “2022-2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi Farmoni, 2007-yil 3-apreldagi PQ-614-son “O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida”gi, 2023-yil 31-maydagi PQ-167-son “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” Qarorlari hamda mazkur faoliyatga tegishli boshqa me’yoriy-huquqiy xujjatlarda belgilangan vazifalarni amalga oshirishga ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Dissertatsiya mavzusi bo‘yicha xorijiy ilmiy-tadqiqotlar sharhi[3]**..**

Axborotni himoyalashning kriptografik usullari, simmetrik shifrlash algoritmlarini yaratish va ularni kriptotahlil usullariga baholash, simmetrik va ochiq kalitli shifrlash algoritmlarini yaratish, kriptobardoshliligini baholash bo‘yicha ilmiy izlanishlar dunyoning yetakchi ilmiy tadqiqot markazlari va oliy ta’lim muassasalari, jumladan, Milliy standartlar va texnologiyalar instituti (NIST) (AQSH), Milliy xavfsizlik agentligi (NSA) (AQSH), Yevropa telekommunikatsiya standartlari instituti (ETSI) (Fransiya), Xalqaro standartlashtirish tashkiloti (ISO) (Shveytsariya), Elektr va elektronika muhandislari instituti (IEEE) (AQSH), “UNICON.UZ” MChJ (O‘zbekiston), Massachusets texnologiya instituti (AQSH), Stenford universiteti (AQSH), Kaliforniya universiteti (AQSH), Karnegi Mellon universiteti (AQSH), Oksford universiteti (Buyuk Britaniya), Kembrij universiteti (Buyuk Britaniya), Syurix federal texnologiya instituti (Shveytsariya), Lozanna federal politexnika maktabi (Shveytsariya), Myunxen texnika universiteti (Germaniya), Leven katolik universiteti (Belgiya), Singapur milliy universiteti

[2] O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” gi PQ-293 sonli Qarori

[3] www.elsevier.com, www.springernature.com, www.ieee.org, www.acm.org, www.wiley.com, www.tandfonline.com, www.mdpi.com, www.worldscientific.com, www.siam.org, www.ams.org, www.ems.press, www.ioppublishing.org, www.nature.com, www.science.org, www.doaj.org, www.scopus.com, www.webofscience.com

(Singapur), Sinxua universiteti (Xitoy), Pekin universiteti (Xitoy), Tokio universiteti (Yaponiya), Koreya ilg‘or fan va texnologiyalar instituti (Janubiy Koreya), Tel-Aviv universiteti (Isroil), Veytsman fan instituti (Isroil), Hindiston texnologiya instituti (Hindiston), Nanyan texnologiya universiteti (Singapur), Rossiya Fanlar Akademiyasi (Rossiya), Moskva davlat universiteti (Rossiya), Sankt-Peterburg davlat universiteti (Rossiya), Belarus davlat universiteti (Belarus), Qozog‘iston Milliy universiteti (Qozog‘iston), Qirg‘iziston-Turkiya Manas universiteti (Qirg‘iziston), Tojikiston Milliy universiteti (Tojikiston), Ozarbayjon Milliy Fanlar Akademiyasi (Ozarbayjon), Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti (O‘zbekiston), Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti qoshidagi Raqamli texnologiyalar va axborot texnologiyalar markazi (O‘zbekiston) va Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti (O‘zbekiston)da olib borilmoqda.

Axborotni himoyalashning kriptografik usullari, simmetrik shifrlash algoritmlarini yaratish va ularni kriptotahlil usullariga baholash, simmetrik va ochiq kalitli shifrlash algoritmlarini yaratish, kriptobardoshliligini baholashga oid dunyoda olib borilgan tadqiqotlar natijasida quyidagi natijalar olingan: simmetrik shifrlash algoritmlari, ularning S-bloklari va chiziqsiz akslantirishlari asosida yangi konstruksiyalar ishlab chiqish, ularning xavfsizligi matematik jihatdan sinovdan o‘tkazish, ochiq kalitli shifrlash algoritmlarini kriptografik baholash va amaliy tizimlarda qo‘llanilishi bo‘yicha nazariy va amaliy natijalar olingan va isbotlangan. Masalan, Rossiya va AQSHdagi ilmiy markazlar va universitetlarda simmetrik shifrlash algoritmlarini tahlil qilish orqali ularning zaif tomonlarini aniqlash va optimallashtirish bo‘yicha tadqiqotlarni amalga oshirilgan; AQSH, Xitoy va Yaponiya universitetlarida post-kvant kriptografiya algoritmlari va kriptotahlil usullari tadqiq qilingan; ochiq kalitli shifrlash va elektron raqamli imzo algoritmlari sohasida Germaniya, AQSH va Shveysariya kabi mamlakatlar tadqiqot markazlarida matematik modellar ishlab chiqilgan, kalit uzunliklari va xavfsizlik parametrlari baholangan; Fransiya va Italiya universitetlarida esa amaliy tizimlarda elektron raqamli imzo va kriptografik protokollarni sinash bo‘yicha ishlanmalar amalga oshirilgan. Kriptotahlil usullarini rivojlantirish bo‘yicha Janubiy Koreya, Isroil, AQSH, Rossiya va Hindiston ilmiy markazlarida algebraik hujumlar, differensial va chiziqli tahlil, yon kanal hujumlariga qarshi himoya mexanizmlari ishlab chiqilgan. Rossiya Fanlar Akademiyasi S.L. Sobolev nomidagi Matematika instituti, Hisoblash matematikasi va matematik geofizika instituti, Ufa ilmiy markazining hisoblash markazli Matematika instituti hamda Moskva va Sankt-Peterburg davlat universitetlarida simmetrik va ochiq kalitli shifrlash algoritmlari hamda ularning kriptobardoshliligi bo‘yicha keng ko‘lamli ilmiy tadqiqotlar olib borilgan. Bu boradagi tadqiqotlar AQSH, Buyuk Britaniya, Rossiya, Shveytsariya, Germaniya, Italiya, Xitoy, Yaponiya, Janubiy Koreya universitetlarida va ilmiy markazlarda olib borilmoqda, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti (O‘zbekiston), “UNICON.UZ” MChJ (O‘zbekiston), Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti qoshidagi Raqamli texnologiyalar va axborot texnologiyalar markazi (O‘zbekiston) va Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti (O‘zbekiston)da olib

borilmoqda.

Dunyoda simmetrik va ochiq kalitli shifrlash algoritmlarini baholash usullari va algoritmlari bo‘yicha ilmiy tadqiqotlar davom etmoqda, bu tadqiqotlarda simmetrik shifrlash algortimlarini kriptotahlil usullariga baholashda va ularning chiziqsiz akslantirishlarini yaratishda umumiy kriptografik talablarga baholash, baholash jarayonida yangi yondashuvlardan foydalanish, ochiq kalitli shifrlash algoritmlarini baholashda yangi usullarni ishlab chiqish, jumladan, faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarida maxfiy va ochiq kalitlar munosabatlari orqali maxfiy kalitlar va parametrlarni aniqlashga asoslangan usullar va algoritmlarni yaratish, yangi yondashuvlarni qo‘llagan holda faktorlashning usul va algoritmlarini ishlab chiqish kabi ustuvor yo‘nalishlar o‘rganilmoqda.

Muammoning o‘rganilganlik darajasi. Axborotning kriptografik himoyasi, simmetrik shifrlash algoritmlarini yaratish, ularni kriptotahlil usullariga baholash bo‘yicha B. Shnayer, K. Shennon, E. Biham, H. Feistel, M. Matsui, J. Daeman, D. Knut, S. Maitra, A. Youssef, N. Tokereva, O. Rothaus, X. Zhang, A. Webster, Y. Liu, L. Brown, V. Parihar, A. Sorkin, X. Zhu, A. Biryukov, M. Dawson, S. Fischer, K. Zamli, N. Siddiqui, M. Spain, C. Carlet, W. Meiyer, W. Stallings, C. Pomerance, J. Ding, M. Kavut, I. Yilmaz, T. Kasami, S. Tavares, Y. Yang, W. Zang, Y. Wang, M. Ahmad, L. Babenko, E. Ishukova, E. Maro kabil olimlar tomonian, turli murakkabliklarga asoslangan ochiq kalitli shifrlash algoritmlarini ishlab chiqish va ularni baholash bo‘yicha R. Rivest, A. Shamir, L. Adleman, N. Koblitz, M. Pollard, A. Lenstra, R. Leman, J. Dixon, A. Joux, K. Lauter, M. Morrison, C. Pomerance, P. Montgomery kabi olimlar tomonidan tadqiqotlar olib borilgan.

Respublikamizda P.F.Xasanov, M. Aripov, M. Karimov, S. Ganiev, B. Abduraximov, A. Kabulov, D. Akbarov, X. Xasanov, O. Axmedova, G. Jo‘rayev, D. Kuryazov, G‘. To‘ychiyev, B. Axmedov, A.Sattorov, Z. Xudoyqulov. O. Allanov, M. Berdimorudov, U. Mardiyev kabi tadqiqotchilar tomonidan axborotni himoyalashning kriptografik usullari, xesh funksiyalar, simmetrik va ochiq kalitli shifrlash algoritmlasrini, elektron raqamli imzo algoritmlarini yaratish, kriptobardoshliligini baholashga oid ilmiy tadqiqotlar olib borilgan.

Kriptotahlil usullari yordamida baholash masalalari bir qator olimlar, jumladan, A. Biryukov, N. Courtois, M. Matsui, M. Pollard, A. Lenstra, R. Leman, J. Dixon, A. Joux, L. Babenko, M. Aripov, B. Abduraximov, G. Jo‘rayev, D. Kuryazov, A.Sattarov, M. Berdimurodov va boshqalarning ilmiy ishlarida ko‘rib chiqilgan. Shu bilan bir qatorda, simmetrik oqimli shifrlash algoritmlarining chiziqsiz akslantirishlarini baholash va shifrlash kalitlarini aniqlashda zamonaviy texnologiyalarning qo‘llanilishi hamda ochiq kalitli shifrlash algoritmlarining maxfiy kalitlarini aniqlashning yangicha yondashuvlari masalalariga yetarlicha e’tibor qaratilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universitetining F-OT-2021-248 “Funksional jadvallar

asosida axborotlarni himoyalash uchun xavf-xatarlarni aniqlash, identifikatsiya va bartaraf qilishning intellektual usullari va texnologiyalarini ishlab chiqish” nomli fundamental loyihasi va AL-9624115223 “Kriptografiya fani bo‘yicha elektron o‘quv qo‘llanma yaratish” nomli amaliy tadqiqot loyihasi doirasida bajarilgan.

Tadqiqotning maqsadi simmetrik va ochiq kalitli shifrlash algoritmlari xavfsizligini baholash uchun yangi yondashuvlar asosida yechimlar ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholashning yangi usulini ishlab chiqish;

simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholashning yangi usuli asosida algoritm yaratish;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun yangi faktorlash usulini ishlab chiqish;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun yangi faktorlash usuli asosida algoritm yaratish;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlash usulini ishlab chiqish;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning yangi usulini ishlab chiqish va bu usul asosida yaratish.

Tadqiqotning ob’yekti sifatida simmetrik va ochiq kalitli shifrlash algoritmlari olingan.

Tadqiqotning predmetini simmetrik va ochiq kalitli shifrlash algoritmlarining kriptobardoshligini baholash usullari tashkil etadi.

Tadqiqotning usullari. Tadqiqot jarayonida amaliy kriptografiya va kriptotahlil usullari, sonlar nazariyasi, ehtimollar nazariyasi, qiyosiy taqqoslash va ob’yektga yo‘naltirilgan dasturlash yordamida tajribalar o‘tkazish usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

S-box akslantirishlarini baholashda mavjud umumiy kriptografik talablarga qo‘shimcha talab sifatida xizmat qiladigan chiziqsiz akslantirishlarga kirish bitlarining birgalikda kelishlari chiqishda qanday tartibda takrorlanishiga asoslangan holda shifrlash kalitlarini aniqlash imkonini bergan simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholash usuli ishlab chiqilgan;

4×4 o‘lchamli S-box akslantirishlariga mos maxfiy kalitning 75 foizini, ayrim S-boxlar uchun esa 100 foiz aniqlik bilan taxmin qilish imkonini bergan simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholash usuli asosida shifrlash kalitini aniqlash algoritmlari yaratilgan;

sonlarni ko‘paytirishdagi munosabatlar orqali faktorlash imkonini bergan sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan ko‘paytirish amallariga teskari amallar orqali faktorlash usuli ishlab chiqilgan;

$2^{\frac{l}{2}-2}$ xotirani ta’minlash imkoniyati mavjud bo‘lganda l bitli RSA ochiq kalitli shifrlash algoritmining modulini faktorlash imkonini bergan sonlarni

ko‘paytirishning Tom-Kuk usuliga asoslanib ishlab chiqilgan usuli asosida yangi faktorlash algoritmlari yaratilgan;

p va q tub sonlarning qaysi intervallarga tegishli bo‘lishi mumkinligining muvaffaqiyatli taxminlarida maxfiy kalitni aniqlash imkonini bergan faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitni aniqlashning maxfiy va ochiq kalitlar munosabatiga asoslangan kichik razryadli RSA modullarida samarali hisoblangan usul ishlab chiqilgan;

RSA ochiq kalitli shifrlash algoritmining moduli l bit bo‘lganda, $|p-q| \le 2^{\frac{l}{4}}$ shart bajarilganda $\frac{l}{2}$ qadam bilan maxfiy kalitlarni aniqlash imkonini bergan faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlash usuli ishlab chiqilgan va mazkur usul asosida algoritm yaratilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholashning “Bitlarning birgalikda kelishlari soni” deb nomlangan yangi usuli asosida ishlab chiqilgan baholash algoritmning dasturiy vositasi ishlab chiqilgan;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan yangi faktorlash usuli asosida faktorlash algoritmining dasturiy vositasi ishlab chiqilgan;

faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning oraliqlarga bo‘lishga asoslangan usuli asosida algoritm ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi. Dissertatsiyada olingan natijalarning ishonchliligi undagi matematik mulohazalarning qat’iyligi, o‘tkazilgan sonli tadqiqot natijalari bilan tasdiqlanganligi hamda yangi ishlab chiqilgan usul va algoritmlarni shifrlash algoritmlariga qo‘llash orqali olingan real hamda tajribaviy natijalar bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati ishlab chiqilgan chiziqsiz akslantirishlarni baholash usulini mazkur turdagi akslantirishlarni ishlab chiqishda, faktorlash muammosiga asoslangan algoritmlarda maxfiy kalit parametrlarini generatsiya qilishda foydalanish mumkinligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati ishlab chiqilgan usul va algoritmlar uchun yaratilgan dasturiy vositalardan mavjud ochiq kalitli shifrlash algoritmlarini hamda shifrlash algoritmlarining chiziqsiz akslantirishlarini baholashda foydalanish mumkinligi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. “Simmetrik va ochiq kalitli shifrlash algoritmlarini baholash usullari va algoritmlari” mavzusidagi tadqiqot ishida olingan ilmiy natijalar asosida:

S-box akslantirishlarini baholashda mavjud umumiy kriptografik talablarga qo‘shimcha talab sifatida xizmat qiladi chiziqsiz akslantirishlarga kirish bitlarining birgalikda kelishlari chiqishda qanday tartibda takrorlanishiga asoslangan holda shifrlash kalitlarini aniqlash imkonini bergan simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholash usulidan JSKY2021098-raqamli “SM4

algoritmini tadqiq etish” nomli loyihada SM4 simmetrik shifrlash algoritmining S-boxi tahlili va baholashda foydalanilgan (Jining Normal Universitetining 15.10.2025 yildagi 20251015-001-sonli ma’lumotnomasi). Natijada, SM4 algoritmi S-box akslantirishini baholash jarayonida NCOB xossasi asosida chetga chiqishlar aniqlangan, jumladan, kirish bitlarining 0- va 2-tartiblari 1,0 ko‘rinishida bo‘lganda, chiqish bitlarining 0- va 2-tartiblari 0 va 1 qiymatlarida kelishlari soni 10 ta, kirish bitlari 0- va 2-tartiblari 1,0 ko‘rinishida bo‘lganda esa chiqish bitlarining 0- va 2-tartiblari 1 va 1 qiymatlarida kelishlari soni 24 ta ekanligi aniqlangan, natijalar oxirgi raund kalitining mos bitlarini 75% gacha aniqlik bilan taxmin qilish imkonini bergan;

$2^{\frac{l}{2}-2}$ xotirani ta’minlash imkoniyati mavjud bo‘lganda *l* bitli RSA ochiq kalitli shifrlash algoritmining modulini faktorlash imkonini bergan sonlarni ko‘paytirishning Tom-Kuk usuliga asoslanib ishlab chiqilgan usuldan xorijiy ilmiy jurnallarda (Journal of Machine and Computing, 05(03), 2025, pp.1944-1957; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp.842-862; Symmetry, 16, 2024, ID 764) Shor algoritmining Qiskit platformasi tomonidan taqdim etilgan simulyatsiya qilingan kvant backendlaridan foydalangan holda keng qamrovli samaradorlik tahlili o‘tkazishda foydalanilgan. Natijada, butun sonlarni faktorlash uchun moslashuvchan va umumiy realizatsiya taklif etilib, unda faktorlanuvchi sonni dinamik kiritish, tasodifiy o‘zaro tub sonlarni tanlash hamda kvant sxemalarni avtomatik shakllantirish imkonini bergan;

chiziqsiz akslantirishlarga kirish bitlarining birgalikda kelishlari chiqishda qanday tartibda takrorlanishiga asoslangan holda shifrlash kalitlarini aniqlash imkonini bergan simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholash usuli va uning asosida yaratilgan shifrlash kalitini aniqlash algoritmlaridan xorijiy ilmiy jurnallarda (Discover Internet of Things, 5, 2025, pp.1-20; Multimedia Tools and Applications, 8, 2024, pp.24859–24886; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp.842-862) ma’lumotlarni uzatish uchun tezkor va barqaror xavfsizlik tizimini yaratishda, optimal talablar bo‘yicha yo‘riqnomalarni ishlab chiqish hamda IoT parametrlariga asoslangan va NIST kriptografik standartlariga tayanuvchi matematik bog‘lanish-modelini yaratishda, graf nazariyasiga asoslangan shifrlash va deshifrlash usullaridan foydalanish orqali kriptografik protokollarni rivojlantirishda foydalanilgan Natijada, taklif etilgan usul va algoritmlardan foydalanib ishlab chiqilgan algoritm an’anaviy Trivium usuliga nisbatan ustunligi, shifrlash va deshifrlash vaqtlari 1:24 nisbatda qisqarganligi, bu uni tezkor xavfsizlik talablariga mos qilishi, yengil vaznli IoT infratuzilmalari uchun moslashtirish mumkinligi ko‘rsatilgan hamda Dekart ko‘paytmasi graflari hamda to‘liq bipartit graflardan foydalanish aloqa tizimlarida ma’lumotlarning maxfiyligi va yaxlitligini oshirishga imkon bergan;

chiziqsiz akslantirishlarga kirish bitlarining birgalikda kelishlari chiqishda qanday tartibda takrorlanishiga asoslangan holda shifrlash kalitlarini aniqlash imkonini bergan simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholash usulidan “Elektron raqamli imzo bulutli xizmatini ishlab chiqish” loyihasida raqamli imzo algoritmlarining parametrlarini generatsiya qilishda va

kriptografik algoritmlarning bardoshliligini baholashda foydalanilgan (“UNICON.UZ” Fan-texnika va marketing tadqiqotlari markazi ma’suliyati cheklangan jamiyatining 29.01.2026 yildagi 7-2/211-sonli ma’lumotnomasi). Natijada, faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning oraliqlarga bo‘lishga asoslangan usul kriptografik bardoshli kalitlarni generatsiya qilishda ularni tizimli baholash imkonini bergan, simmetrik shifrlash algoritmlarining chiziqsiz akslantirishlarini baholashning “Bitlarning birgalikda kelishlari soni” deb nomlangan yangi usul kriptografik algoritmlarning bardoshliligini baholash imkonini bergan.

Tadqiqot natijalarining approbatsiyasi. Mazkur tadqiqot natijalari 16 ta ilmiy-amaliy anjumanlarda, jumladan, 4 ta xalqaro va 12 ta respublika ilmiy-amaliy anjumanlarda muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiya mavzusi bo‘yicha jami 43 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish uchun tavsiya etilgan ilmiy nashrlarida 20 ta maqola, shundan, 11 tasi xorijiy (9 ta maqola Scopus bazasiga indekslangan) va 9 tasi respublika jurnallarida nashr etilgan. Shuningdek, EHM uchun yaratilgan 7 ta dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, besh bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 153 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida o‘tkazilgan tadqiqotlarning dolzarbligi va zarurati, tadqiqotning respublika fan va texnologiyalari rivojlantirishning ustuvor yo‘nalishlariga mos kelishi asoslangan. Dissertatsiya mavzusi bo‘yicha chet eldagi ilmiy tadqiqotlarning qisqacha ma’lumoti va muammoning o‘rganilganlik darajasi keltirilgan, tadqiqotning maqsadi va vazifalari, obyekt va predmetlari ko‘rsatilgan, tadqiqotning ilmiy yangiligi va amaliy natijalari bayon qilingan, olingan natijalarning ilmiy va amaliy ahamiyati ochib berilgan, tadqiqot natijalarini amaliyotga joriy qilish, nashr etilgan ishlar va dissertatsiya tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning birinchi bobi “**Zamonaviy kriptografik algoritmlarni baholash usullari**” deb nomlangan bo‘lib, zamonaviy kriptografik tizimlarning asosiy yo‘nalishlarini tashkil etuvchi simmetrik va ochiq kalitli shifrlash algoritmlarini baholash usullari keng tahlil qilingan. Tadqiqot jarayonida har ikki turdagi shifrlash tizimlarining matematik asoslari, ularning xavfsizlik mezonlari hamda baholash metodologiyalari o‘rganilib, ularning afzallik va cheklovlari ilmiy nuqtayi nazardan umumlashtirilgan. Bobning birinchi paragrafi **“Simmetrik shifrlash algoritmlari va ularning chiziqsiz akslantirishlarini baholash usullari”** deb nomlangan bo‘lib, unda simmetrik shifrlash algoritmlarining chiziqsiz akslantirishlarini tahlil qilish usullari, jumladan, chiziqlilik darajasi, algebraik

immunitet, differensial va chiziqli kriptotahlilga bardoshlilik, hamda S-box chiziqsizligi mezonlari asosida baholash mexanizmlari ko‘rib chiqildi. Ushbu usullar algoritmlarning ichki blok tuzilmasi, raundlar soni, va kalit uzunligi bilan chambarchas bog‘liqligi aniqlanib, ularning o‘zaro ta’siri matematik jihatdan izohlangan.

Bobning ikkinchi paragrafi “Ochiq kalitli shifrlash algoritmlarini baholash usullari” deb nomlangan bo‘lib, unda ochiq kalitli shifrlash algoritmlarining xavfsizlik baholash usullari ko‘rib chiqilib, ularning matematik negizi bo‘lgan faktorlash, diskret logarifm, hamda elliptik egri chiziq muammolari tahlil qilindi. Ayniqsa, RSA, El-Gamal, va ECC algoritmlarining xavfsizligi asosida yotuvchi matematik masalalarning hisoblash murakkabligi va ularning yechilishiga ta’sir etuvchi zamonaviy algoritmik yondashuvlar (Pollard rho, Quadratic Sieve, ECM, GNFS) o‘rganildi. Shuningdek, kvant hisoblash modellari paydo bo‘lishi bilan bu algoritmlarning xavfsizlik darajasi qayta ko‘rib chiqilayotgani ta’kidlandi.

Chekli maydondagi diskret logarifmlash va elliptik egri nuqtasining tartibini aniqlash bo‘yicha ayrim asosiy algoritmlar to‘g‘ridan-to‘g‘ri faktorlash muammosiga yoki faktorlash usullarining printsipiga tayanganligi sababli, faktorlash usullari asosiy e’tiborda bo‘lishi mantiqiy. Faktorlash metrikalari (smoothness, subproduct daraxtlar, L-notationdagi murakkablik) DLP/EECh-tartib metodlarining samaradorligini belgilashda markaziy rol o‘ynaydi, shuning uchun avvalo faktorlash algoritmlari (Pollard-rho, ECM, QS, NFS va boshqalar) bilan chuqur tanishish ekvivalent yoki undan muhim bosqich hisoblanadi. Shu sababli mazkur bo‘limda faktorlash usullari batafsil yoritildi, DLP va EECh-tartib metodlari esa ularning faktorlashga bog‘liqligi nuqtai nazaridan qisqacha ta’riflangan.

Bobning uchinchi paragrafi “Simmetrik va ochiq kalitli shifrlash algoritrmlarini baholashning dolzarb muammolari” deb nomlangan bo‘lib, unda simmetrik va ochiq kalitli shifrlash algoritmlarini baholashdagi dolzarb muammolar tahlil qilingan. Xususan quyidagilar aniqlangan: mavjud baholash usullari ko‘pincha nazariy mezonlar bilan cheklanib, amaliy samaradorlikni to‘liq aks ettirmasligi, shifrlash algoritmlarining parametrik optimallashtirilgan modellarini yaratish imkoniyati yetarli o‘rganilmaganligi, mashinaviy o‘qitish va neyron tarmoqlar asosida baholash yondashuvlari hali to‘liq tizimlashtirilmaganligi. Shuningdek, simmetrik algoritmlar uchun chiziqsiz akslantirishlarni tahlil qilish va ochiq kalitli algoritmlar uchun faktorlash muammosiga asoslangan baholash usullarini takomillashtirish zaruriyati ilmiy asoslangan.

1-bob natijalari shuni ko‘rsatganki, mavjud baholash yondashuvlari kriptotizimlarning faqat alohida xususiyatlarini o‘lchashga qaratilgan bo‘lib, integrallashgan, adaptiv va intellektual yondashuvlarga ehtiyoj yuqori. Shu sababli, keyingi boblarda ushbu muammolarni bartaraf etish maqsadida yangi baholash usullari, chiziqsiz akslantirishni tahlil qilishning yangi usuli va algoritmlari, mashinali o‘qitish usullari yordamida shifrlash kalitlarini tasniflash usuli va algoritmi hamda faktorlash muammosi asosida qurilgan ochiq kalitli shifrlash

algoritmlarining maxfiy kalitlarini aniqlash algoritmlari ishlab chiqishga qaratilgan usullar va algoritmlar taklif etilgan.

Dissertatsiyaning ikkinchi bobi "**Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishlarini baholashning BBKS usuli va algoritmi**" deb nomlangan bo'lib, unda simmetrik shifrlash algoritmlarining chiziqsiz akslantirishlarini baholash uchun yondashuvlar, chiziqsiz akslantirishlari uchun qo'yilgan umumiy xarakteristik talablar o'rganilgan, ularga qo'shimcha akslantirishdagi kirish va chiqish bitlarining birgalikda paydo bo'lishlarining statistik xarakteristikalariga asoslangan "Bitlarning birgalikda kelishlari soni" deb nomlangan usul taklif qilingan va ushbu usul asosida algoritm ishlab chiqilgan. Ishlab chiqilgan algoritm yordamida Magma shifrlash algoritmining 8 ta chiziqsiz akslantirish jadvalllari baholangan.

Bobning birinchi paragrafi "Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishlarini baholashning mavjud yondashuvlari" deb nomlangan bo'lib, unda simmetrik shifrlash algoritmlarin baholashning mavjud yondashuvlari va chiziqsiz akslantirishlarning xarakteristikalarini tahlil qilish mezonlari o'rganilgan. Simmetrik shifrlash algoritmlari har qanday kriptografik almashtirishlarini $GF(2^n)$ fazodagi $X = (x_1, x_2, \dots, x_n)$ ni, boshqa $GF(2^m)$ fazodagi $Y = (y_1, y_2, \dots, y_n)$ ga akslantirish sifatida qarab, ushbu akslantirishni bul funksiyalar orqali quyidagicha ifodalash mumkin: $= \varphi(X)$: $GF(2^n) \to GF(2^m), X = (x_1, x_2, \dots, x_n), Y = (y_1, y_2, \dots, y_n)$.

Akslantirish esa $\varphi(X) = \{f_1(X), f_1(X), \dots, f_m(X)\}$ – vektor bul funksiyalar (komponentalar) ko'rinishida tasvirlanadi. Bu yerda $f_i, x_i, y_i \in GF(2)$ $(f_i, x_i, y_i = \{0,1\}$. Demak, blokli simmetrik shifrlash algoritmidagi biror kriptografik almashtirishni baholash jarayonida unga matematik model bo'lgan, berilgan bul funksiya xossalarini o'rganish yetarli hisoblanadi.

Mazkur keltirilgan tushunchalardan ma'lumki, blokli simmetrik shifrlash algoritmi almashtirishlarining yuqorida keltirilgan barcha xossalari va sonli xarakteristikalari ushbu shifrlash algoritmining kriptobardoshliligiga o'z ta'sirini ko'rsatadi.

Bobning ikkinchi paragrafi "Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli" deb nomlangan. Mazkur bo'limda S-box akslantirishining avval mavjud bo'lgan umumiy xarakteristikalariga qo'shimcha ravishda, kiruvchi va chiquvchi bitlarning birgalikda paydo bo'lish ehtimolligini o'rganishga asoslangan yondashuv taklif qilingan. Bu yondashuvlar yordamida S-box ichidagi bitlar orasidagi bog'liqlik darajasi aniqlanadi.

BBKS usulining mazmunini quyidagi 1-ta'rif bilan ifodalash mumkin.

1-ta'rif. Faraz qilaylik, S -o'lchami $n \times n$ bo'lgan S-box bo'lib, kiruvchi qiymat $a \in \{0,1\}^n$ ni, chiquvchi qiymat esa $b = S[a] \in \{0,1\}^n$ ni ifodalaydi. U holda bitlarning birgalikda paydo bo'lishlari soni quyidagicha aniqlanadi:

$$c_{p,q}^{i,j}[k,l] = \#\{b_k = p; b_l = q; a_k = i; a_l = j\}$$

Bu yerda $k = 0, \dots, n-2; l = k+1, \dots, n-1$, $p = 0,1;\ q = 0,1;$ $i = 0,1; j = 0,1.$

BBKS usuli - S-box chiziqsiz akslantirishlarini baholash bosqichlari

1-bosqich. Kirish ma'lumotlarini tayyorlash. Olchami $n \times n$ boilgan S-box jadvali tanlanadi. S-boxdagi har bir kinuvchi qiymat $a \in \{0,1\}^n$ va unga mos chiquvchi qiymat $b = S[a] \in \{0,1\}^n$ aniqlanadi. Barcha qiymatlar ikkilk (binary) ko'rinishda ifodalanadi.

2-bosqich. Bit juftliklarini aniqlash. Har bir kiruvchi qiymatdagi bitlar juftligi (a_k, a_l) uchun barcha mumkin bo'lgan $(i,j) \in \{0,1\}^2$ kombinatsiyalar olinadi. Shunga mos ravishda chiquvchi qiymatdagi bitlar juftigi (b_k, b_l) uchun $(p,q) \in \{0,1\}^2$ qiymatlar tanlanadi. Bu jarayon barcha k, l indeks juftliklari uchun (ya'ni $= 0, \dots, n-2; l = k+1, \dots, n-1$) amalga oshiriladi.

3-bosqich. Birgalikda paydo bo'lishlar sonini hisoblash. Har bir bit juftligi kombinatsiyasi uchun quyidagi miqdor hisoblanadi:

$$c_{(p,q)]}^{(i,j)}[k,l] = \#\{b_k = p; b_l = q; a_k = i; a_l = j\}$$

Bu kattalik kirishdagi $(a_k, a_l) = (i,j)$ juftliklari chiqishdagi $(b_k, b_l) = (p,q)$ juftliklariga qanchalik ko'p mos tushishini bildiradi.

4-bosqich. Ehtimolliklarni hisoblash. Har bir qiymat uchun ehtimollik aniqlanadi:

$$P_{(p,q)}^{[i,j]}[k,l] = \frac{c_{(p,j)}^{(i,j)}[k,l]}{2^u}$$

Bu ifoda kirish-chiqish bitlari orasidagi statistik bogliqlik darajasini ehtimollik shaklida ifodalaydi.

5-bosqich. Natijalarni tahlil qilish. Agar barcha $P_{(pq)}^{(i,j)}[k,l]$ qiymatlar bir-biriga yaqin bo'lsa, demak S-box ichidagi bitlar mustaqil va teng taqsimlangan, bu esa yuqori chiziqsizlik va bardoshlilikni bildiradi. Aksincha, ayrim juftliklarda $P_{(p,q)}^{(i,j)}[k,l]$ qiymati juda katta yoki kichik bo'lsa, bu bitlararo o'zaro bog'liqlik mavjudligini va S-boxning kriptoanalitik zaifligini ko'rsatadi.

Natijalar S-boxni takomillashtirish, yangi S-baxlarni ishlab chiqish yoki mavjudlarini optimallashtirishda qo'llanadi.

2.1-Lemma (BBKS usulida bit-juftliklarning teng taqsimlanish xossasi). Faraz qilaylik, $S: \{0,1\}^n \to \{0,1\}^n -$ S-box. Agar har bir kirish qiymat $a \in \{0,1\}^n$ uchun chiqish qiymat $b = S[a]$ mavjud bo'lib, barcha bit juftliklar (a_k, a_l) va (b_k, b_l) kombinatsiyalari teng chastotada uchrasa, ya'ni

$$\sum_{a \in \{0,1\}^n} [a_k = i, a_l = j, b_k = p, b_l = q] = \frac{2^{n-2}}{4}$$

u holda shu juftliklar bo'yicha taqsimot bir xil hisoblanadi.

2.1-Teorema (BBKS usulida bitlarning mustaqillik sharti). Agar 2.1-lemma sharti bajarilsa, ya'ni har bir (i, j, p, q, k, l) kombinatsiya uchun

$$c_{p,q}^{i,j}[k,l] = \frac{2^{n-2}}{4}$$

bo'lsa, u holda S-boxdagi k-va l-tartibli bitlar o'zaro statistik jihatdan mustaqil bo'ladi.

Bu $4x4$ o‘lchamli Magma shifrlash algoritmining 8 - S-boxida a kirishning 1-tartibli biti 0 ga va 3-tartibli biti 1 ga teng bo‘lganda, b chiqishning 1-tartibli biti 1 ga va 3-tartibli biti 1 ga teng bo‘lishlari soni 3 ga teng ekanligini bildiradi (1-jadval).

1-jadval.

Magma algoritmining 8-S-box jadvalida bitlarning birgalikda kelishlari (BBKS) soni

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	1	0	2	2	1	1	0	0	2	1	1	1	0	2	1
0,2	**3**	1	0	0	0	1	2	1	1	0	2	1	0	2	0	2
0,3	1	1	2	0	0	**3**	0	1	1	0	1	2	2	0	1	1
1,2	1	0	1	2	0	1	1	2	2	0	2	0	1	**3**	0	0
1,3	1	1	2	0	0	0	1	**3**	2	2	0	0	1	1	1	1
2,3	2	2	0	0	1	1	0	2	1	0	2	1	0	1	2	1

BBKS usuli S-boxlarning chiziqsiz akslantirish xossalarini tahlil qilishda yangi, bit darajasidagi yondashuvni taklif etadi. An’anaviy algebraik, differensial yoki chiziqli tahlil usullari ko‘proq S-boxning umumiy tuzilishiga qaratilgan bo‘lsa, BBKS yondashuvi kiruvchi va chiquvchi bitlar o‘rtasidagi birgalikda paydo bo‘lish ehtimolligini baholash orqali ichki bog‘liqlik darajasini aniqlaydi. Bu esa S-boxning statistik mustaqilligi va tarqatish xususiyati haqida chuqurroq ma’lumot beradi. Agar bitlararo bog‘liqlik minimal darajada bo‘lsa, bunday S-box nisbatan yuqori bardoshlilikni namoyon etadi.

Bobning uchinchi paragrafi “Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 1-algoritm” deb nomlangan va unda simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 1-algoritm tasvirlangan.

1-algoritm. Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 1-algoritm

1-qadam. Tasodifiy kirish qiymatlari uchun bir qancha shifrlash jarayoni amalga oshiriladi. Jarayon S-boxga mos bitlar uchun L_n, R_n qabul qilishi mumkin bo‘lgan barcha variantlari bir martadan qatnashadigan, ya’ni qiymatlari takrorlanmaydigan massiv hosil bo‘lguncha davom ettiriladi. Bunday massivlar shifrlash jarayoni L_{n-1} ning bir xil qiymatida amalga oshirilganda hosil bo‘ladi.

2-qadam. Hosil bo‘lgan R_n massivni S-box sifatida e’lon qilib ushbu S-boxdagi bitlarning birgalikda kelishlari soni aniqlanadi.

3-qadam. Shifrlash jarayonida foydalanilgan S-box jadvalidagi bitlarning birgalikda kelishlari soni ifodalangan jadvaldagi BBKS ning mos qiymatlarini va R_n massiv uchun aniqlangan BBKS qiymatlarini xor amali bilan qo‘shish orqali L_{n-1} ning qiymati aniqlanadi.

4-qadam. Mavjud L_{n-1}, L_n, R_n qiymatlardan foydalanib $L_{n-1} \oplus S(L_n \oplus K_n) = R_n$ ifoda orqali K_n ning qiymati aniqlanadi.

5-qadam. Hosil qilingan K_n ning qiymati taxmin qilingan n-raund kaliti sifatida e’lon qilinadi.

2-jadval.

R_n massiv qiymatlaridan tuzilgan S-box jadvalida bitlarning birgalikda paydo bo‘lishlari soni

	0,0				0,1				1,0				1,1			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	2	1	1	0	1	1	1	1	1	0	2	1	0	2	1	1
0,2	2	0	1	1	1	2	0	1	1	2	1	0	0	0	1	3
0,3	1	1	2	0	1	2	1	0	0	1	0	3	2	0	1	1
1,2	3	1	0	0	0	2	0	2	1	1	1	1	0	1	2	1
1,3	1	1	1	1	2	2	0	0	1	0	0	3	1	1	2	0
2,3	1	1	1	1	2	1	1	0	0	2	1	1	0	0	2	2

1-qadamdagi shartlar asosida amalga oshirilgan hisoblashlar natijasida L_n=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15] va R_n =[8, 1, 6, 3, 12, 0, 5, 14, 9, 2, 15, 10, 7, 4, 13, 11] massivlar hosil bo‘ldi. 2-qadamga asosan R_n massivni S-box sifatida e’lon qilib, ushbu S-boxdagi bitlarning birgalikda paydo bo‘lishlari soni aniqlandi.

4-jadval.

Birgalikda kelishlari soni jadvallaridagi mos qiymatlardan foydalanib L_{n-1} ning qiymatini aniqlash

Bitlarning o‘rni	**S-boxdagi qiymatlari**	**R_n massivdagi mos qiymat**	**Mos qiymatlarning XOR natijasi**	**0-bit**	**1-bit**	**2-bit**	**3-bit**
0,2	0,0	1,1	1,1	1	-	1	-
0,3	0,1	1,1	1,0	1	-	-	0
1,2	0,1	0,0	0,1	-	0	1	-
1,3	1,1	1,1	0,0	-	0	-	0
0,2	0,1	1,0	1,1	1	-	1	-
0,3	1,1	0,1	1,0	1	-	-	0
1,2	0,0	0,1	0,1	-	0	1	-
1,3	1,0	0,0	1,0	-	1	-	0
L_{n-1} ning hosil qilingan qiymati:				**1**	**0**	**1**	**0**

3-qadamga asosan shifrlash jarayonida foydalanilgan S-box jadvalidagi bitlarning birgalikda paydo bo‘lishlari soni ifodalangan {0,2},{0,3},{1,2},{1,3} chiquvchi bitlarga mos keluvchi 2-jadvaldagi qiymatlardan foydalanib L_{n-1} ning qiymati aniqlanadi (3-jadval).

4-qadamga ko‘ra L_{n-1} ning qiymati aniqlangandan so‘ng K_n ning qiymati quyidagi ifoda orqali aniqlanadi:

$$L_{n-1} \oplus S(L_n \oplus K_n) = R_n \qquad (1)$$

Ushbu ifoda L_n massivning ixtiyoriy qiymatlarida va unga mos R_n massiv qiymatlarida o‘rinli hisoblanadi.

Agar $L_n = 0_{10} = 0000_2$ bo‘lsa unga mos R_n massiv qiymati $R_n = 8_{10} = 1000_2$ bo‘ladi. Bu qiymatlarni aniqlangan $L_{n-1} = 10_{10} = 1010_2$ qiymatni (1) ifodaga qo‘yish orqali $1010 \oplus S(0000 \oplus K_n) = 1000$ ifodaga ega bo‘lish mumkin. Bundan esa $S(0000 \oplus K_n) = 0010$ ni va 1-jadval yordamida $K_n = 1111$ kalit qiymati aniqlandi.

Bobning to‘rtinchi paragrafi “Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 2-algoritm” deb nomlangan va unda simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 2-algoritm tasvirlangan.

2-algoritm. Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 2-algoritm

1-qadam. R_n massivning barcha qiymatlari bir xil (masalan, barcha qiymatlar 0 yoki 1) qiymatni qabul qilganda L_n ning mumkin bo‘lgan barcha qiymatlari hosil bo‘lguncha shifrlash jarayoni amalga oshiriladi.

2-qadam. Hosil bo‘lgan L_n massivni S-box sifatida e’lon qilib ushbu S-boxdagi bitlarning birgalikda kelishlari soni aniqlanadi.

3-qadam. Shifrlash jarayonida foydalanilgan S-box jadvaliga teskari S-box_inv uchun bitlarning birgalikda kelishlari soni jadvali shakllantiriladi.

4-qadam. Shakllantirilgan S-box_inv uchun va L_n massiv uchun shakllantirilgan BBKS jadvallarini mos qo‘yish, ya’ni mos bitlarini xor amali orqali qo‘shish yo‘li bilan K_n ning qiymati aniqlanadi.

5-qadam. Hosil qilingan K_n ning qiymati taxmin qilingan n-raund kaliti sifatida e’lon qilinadi.

L_n massivining bitlarining birgalikda paydo bo‘lishlari soni (6-jadval) S-box_inv jadvalining bitlarining birgalikda paydo bo‘lishlari soni (5-jadval) bilan mos qo‘yish orqali shifrlash jarayonidagi kalit aniqlanadi (7-jadval).

5-jadval.

8-S-box jadvaliga teskari S-box_inv jadvalida bitlarning birgalikda paydo bo‘lishlari soni

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	2	0	1	1	1	2	0	0	1	1	2	2	0	1	1
0,2	3	0	1	0	1	1	0	2	0	2	2	0	0	1	1	2
0,3	1	0	1	2	1	3	0	0	2	0	1	1	0	1	2	1
1,2	1	0	2	1	0	1	0	3	1	1	2	0	2	2	0	0
1,3	1	0	2	1	1	0	2	1	2	1	1	0	0	3	0	1
2,3	2	1	1	0	2	1	0	1	0	0	2	2	0	2	1	1

6-jadval.

L_n massivi bitlarning birgalikda paydo bo‘lishlari soni

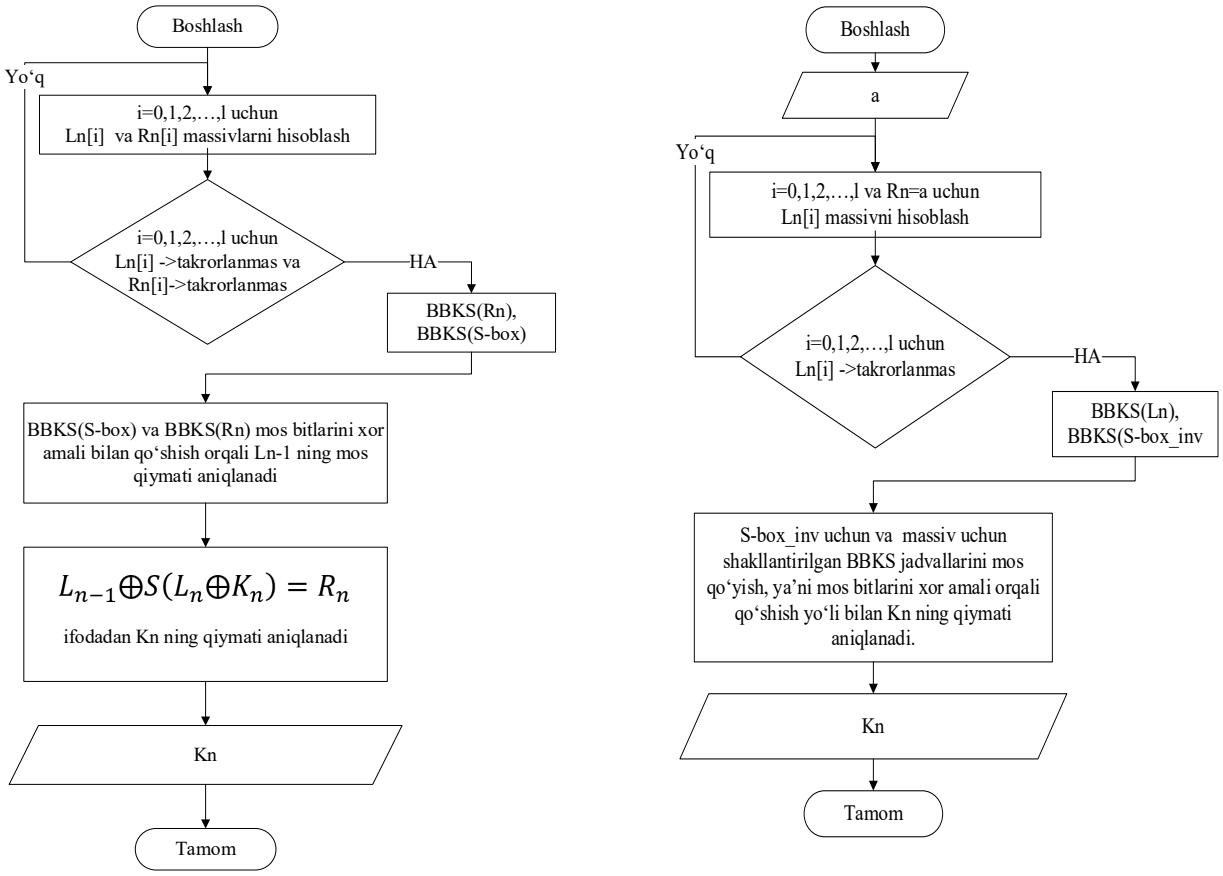
	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	0	2	1	0	2	1	1	2	1	1	0	1	1	1	1
0,2	0	1	0	3	2	0	1	1	0	2	2	0	2	1	0	1
0,3	2	1	0	1	0	0	3	1	1	1	0	2	1	2	1	0
1,2	1	2	0	1	3	0	1	0	0	2	1	1	0	1	1	2
1,3	1	2	0	1	1	2	0	1	1	1	1	1	1	0	3	1
2,3	0	1	1	2	1	0	1	2	2	1	0	1	1	1	2	0

7-jadval.

Birgalikda kelishlari soni jadvallaridagi mos qiymatlardan foydalanib K_n ning qiymatini aniqlash

Bitlarning o‘rni	S_inv-boxdagi qiymatlari	L_n massivdagi mos qiymat	Mos qiymatlarning XOR natijasi	0-bit	1-bit	2-bit	3-bit
0,2	0,0	1,1	1,1	1	-	1	-
0,3	0,1	1,0	1,1	1	-	-	1
1,2	1,1	0,0	1,1	-	1	1	-
1,3	0,1	1,0	1,1	-	1	-	1
0,2	1,0	0,1	1,1	1	-	1	-
0,3	0,0	1,1	1,1	1	-	-	1
1,2	0,1	1,0	1,1	-	1	1	-
1,3	1,1	1,1	0,0	-	0	-	0
K_n ning hosil qilingan qiymati:				**1**	**1**	**1**	**1**

$K_n=1111_2$ shifrlash jarayonida foydalanilgan kalit bitlari ekanligini aniqlash jarayoni murakkab emas.



1-rasm. Simmetrik shifrlash algoritmlarining chiziqsiz akslantirishini baholash uchun BBKS usuli asosida ishlab chiqilgan 1- va 2- algoritmlarning blok sxemasi

Dissertatsiyaning uchinchi bobi “Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirish qoidasi asosida faktorlash usuli va algoritmi” deb nomlangan. Ushbu bobda, sonlarni

ko‘paytirishning tezkor usullari o‘rganilgan va faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan yangi KATAOF faktorlash usuli ishlab chiqilgan. faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan yangi KATAOF faktorlash usuli asosida ikkita KATAOF-1 va KATAOF-2 faktorlash algoritmlari ishlab chiqilgan.

Bobning birinchi paragrafi “Sonlarni ko‘paytirishning tezkor usullari va ularning qo‘llanilishi” deb nomlangan. Sonlarni ko‘paytirish arifmetikaning eng muhim amallaridan biridir. Katta sonlar bilan ishlaganda, ayniqsa kriptografiya, raqamli signalni qayta ishlash, kompyuter grafikasi va algoritmik hisoblashlarda ko‘paytirish tezligi hisoblash samaradorligiga bevosita ta’sir qiladi. Shu sababli, matematika tarixi davomida ko‘paytirishni tezlashtiruvchi ko‘plab matematik usullar ishlab chiqilgan. Mazkur paragrafda Karatsuba, Toom-Cook, Schonhage-Strassen, Harvey & van der Hoeven, Booth kodlash, Wallace va Dadda daraxtlari, GMP/MPIR kabi matematik usullar o‘rganildi.

Sonlarni ko‘paytirishning turli tezkor algoritmlari - Karatsuba, Toom-Cook, Schonhage-Strassen va Furye usullari - matematik jihatdan faqat arifmetik amallarni tezlashtirish uchun emas, balki kriptoanalitik jarayonlarda, xususan, faktorlash (factorization) masalalarida ham nazariy ahamiyat kasb etadi. Chunki faktorlashning markazida N=p×q kabi ko‘paytma yotadi, bu esa teskari yo‘nalishda, ya’ni ko‘paytmani tahlil qilib uning bo‘luvchilarini topishda, ko‘paytirishning tuzilmasi va xossalarini chuqur o‘rganishni talab qiladi.

Natijada, tezkor ko‘paytirish usullari faqat hisoblashni optimallashtiruvchi matematik vosita emas, balki ularni faktorlash va kriptoanaliz kabi murakkab masalalarni yechishda yangi nazariy asos yaratish imkonini beruvchi yo‘nalish sifatida ham qarash mumkin. Shu sababli, raqamlarni ko‘paytirish mexanizmlarini chuqur o‘rganish - zamonaviy kriptotizimlarning ishonchliligini baholash va yangi tezkor faktorlash modellarini ishlab chiqish uchun muhim ilmiy yo‘nalish hisoblanadi.

Bobning ikkinchi paragrafi “Sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan KATAOF faktorlash usuli” deb nomlangan. Dissertatsiya ishining ushbu paragrafida sonlar va ko‘phadlarni ko‘paytirishga asoslangan Tom-Kuk algoritmi qadamlari yordamida faktorizatsiya muammosini yechish imkoniyati o‘rganilgan. Tadqiqot natijalariga asoslanib, faktorizatsiya jarayonini samarali amalga oshirishga yo‘naltirilgan usul va ushbu usul asosida ishlab chiqilgan algoritmlarning qo‘llanilishi yoritilgan.

Sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan KATAOF faktorlash usuli

Kirish ma’lumotlari:

N – factorlanishi zarur bo‘lgan son;

k - sonning bit uzunligi;

l - har bir qismning bit uzunligi;

$m = n/l$ - hosil bo‘ladigan qismlar soni.

1-qadam. Sonni qismlarga ajratish N soni $m = n/l$ ta l-bitli qismlarga ajratiladi:

$$N = [n_{m-1}, n_{m-2}, \dots, n_1, n_0]$$

bu yerda har bir $n_i - N$ sonining l-bitli qismi.

2-qadam. Dastlabki nomzod juftliklarni aniqlash

Izlanayotgan tub sonlar p va q uchun:

$$p = [p_{k/l-1}, \dots, p_1, p_0], q = [q_{k/l-1}, \dots, q_1, q_0]$$

Har bir n_i qiymat uchun ko‘paytirish qoidasiga teskari amallar yordamida mos (p_i, q_i) nomzod juftliklar aniqlanadi.

3-qadam. Nomzod juftliklarni kengaytirish. Aniqlangan boshlang‘ich p_0, q_0 juftliklaridan boshlab, rekursiv tarzda quyidagi juftliklar hosil qilinadi:

$$(p^i, q^i), i = 0,1,2, \dots, 2^{k-2} - 1.$$

Natijada 2^{k-2} ta potensial juftliklar to‘plami hosil qilinadi.

4-qadam. Tenglikni tekshirish. Har bir nomzod juftlik uchun quyidagi shart tekshiriladi:

$$p^i \times q^i = N.$$

Agar tenglik bajarilmasa, keyingi juftlik uchun tekshiruv davom ettiriladi.

5-qadam. Tugatish. Agar ma’lum bir i uchun $p^i \times q^i = N$ tenglik qanoatlantirilsa, unda: $p = p^i, q = q^i$ deb olinadi va ular izlanayotgan tub sonlar deb e'lon qilinadi. Algoritm ishini yakunlaydi.

Chiquvchi qiymatlar: $(p, q) - N$ sonining tub bo‘luvchilari deb e’lon qilinadi.

Bobning uchinchi paragrafi “Sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan KATAOF faktorlash algoritmlari” deb nomlangan. 3.2-paragrafda taklif qilingan sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan faktorlash usuli asosida ikkita k bitli p va q tub sonlar ko‘paytmasi bo‘lgan N sonini faktorlash algoritmini quyidagi ko‘rinishida tasvirlash mumkin.

Sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan faktorlash usuli asosida ishlab chiqilgan KATAOF-1 algoritmining blok sxema ko‘rinishi 2-rasmda keltirilgan.

Sonlarni ko‘paytirishning Tom-Cook usuliga asoslangan faktorlash usuli asosida ishlab chiqilgan KATAOF-2 algoritmining blok sxema ko‘rinishi 3-rasmda keltirilgan.

Tom-Cook ko‘paytirish usuliga asoslangan ushbu faktorizatsiya usuli katta sonlarni tahlil qilishda yangi imkoniyatlar ochadi. Bu yondashuv katta razryadli kriptografik modullarni faktorlash, RSA xavfsizligini baholash, va matematik kriptoanaliz sohalarida amaliy qo‘llanilishi mumkin bo‘lgan istiqbolli usullardan biridir.

Mazkur bobda faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitni aniqlashning maxfiy va ochiq kalitlar munosabatiga asoslangan kichik razryadli RSA modullarida samarali hisoblangan MOKM usuli taklif qilingan. Shuningdek, faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning butun kavdrat ildizlar kavadratining yaqinlashuvi usuli (BKIKYU) deb nomlangan maxfiy kalitlarni aniqlash usuli ishlab chiqilgan va faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning BKIKYU usuli asosida

algoritm ishlab chiqilgan.

Dissertatsiyaning to‘rtinchi bobi “Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun kalitlar munosabatiga asoslangan usullar va algoritm” deb nomlangan.

Bobning birinchi paragrafi “Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy va ochiq kalitlar munosabatiga asoslangan MOKM usuli” deb nomlangan. RSA shifrlash algoritmida berilgan ochiq kalit e va $N = p * q$ sonlari yordamida $p, q \in (a, b)$ $\varphi(N) = (p-1) * (q-1)$ $(p, q \in (a, b))$ maxfiy kalitni aniqlashning MOKM usulining umumiy tavsifi quyida keltirilgan.

4.1-usul. RSA shifrlash algoritmining maxfiy kalitini aniqlashning MOKM usuli.

1. (a, b) intervalni kichik qismlarga ajratiladi;

2. p, q sonlari ajratilgan qismlarning qaysi biriga tegishli bo‘lishi mumkinligi aniqlanadi;

3. 2-qadamda aniqlangan qismlar uchun $r \in [\frac{2\cdot(\left[\frac{N''}{2}\right]-[\sqrt{N''}])-\varphi''(N'')}{2}, \frac{2\cdot(\left[\frac{N'}{2}\right]-[\sqrt{N'}])-\varphi'(N')}{2}]$, $N' = p_{min} \cdot q_{max}$, $\varphi'(N') = (p_{min}-1)\cdot(q_{max}-1), N'' = p_{min} \cdot q_{min}$, $\varphi''(N'') = (p_{min}-1)\cdot(q_{min}-1)$ p_{min}, q_{max} oraliqlar hisoblanadi;

4. r ning 3 – qadamda aniqlangan oraliqdagi qiymatlari yordamida hisoblangan $\varphi(N) = 2 \cdot (\left[\frac{N}{2}\right] - \left[\sqrt{N}\right] - r)$ uchun $m^e \ mod \ n = m^{e+\varphi(N)} \ mod \ N$ tenglik o‘rinli bo‘lsa hisoblashlar to‘xtatiladi;

5. 4-qadamdagi tenglikni qanaoatlantiruvchi $\varphi(N)$ izlanayotgan maxfiy kalit sifatida e’lon qilinadi.

Keltirilgan usul kichik razryadli tub sonlar p va q uchun samarali ishlashini tajribaviy natijalar orqali tasdiqlaydi. Bunda algoritmning mohiyati $N = p \times q$ modulga asoslangan holda, $\varphi(N)$ funksiyasining qiymatini bilvosita aniqlash va mos holda shifrlash-deshifrlash munosabatlarini tekshirishga qaratilgan.

Keltirilgan usulning samaradorligi (a, b) oraliqni imkoni boricha kichik oraliqlarga ajratish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlashga bog‘liq. (a, b) oraliqni kichik oraliqlarga bo‘lish va izlanayotgan p va q sonlarni qaysi oraliqda ekanligini aniqlashning optimal usuli aniqlansa, yoki r sonining N soniga qanday bog‘liqligi aniqlansa mazkur usulning samaradorligi anchagina ortadi.

Bobning ikkinchi paragrafi “Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitlarini aniqlashning BKIKYU usuli” deb nomlangan. Ushbu paragrafda RSA algoritmining xavfsizlik asosini tashkil etuvchi modulning faktorlash murakkabligi o‘rganiladi. Modul $N = p * q$ uzunligi l bit bo‘lganda, agar tub bo‘luvchilar orasidagi farq $|p-q| \leq 2^{l/4}$ shartni qanoatlantirsa, modulni faktorlash odatdagi usullarga nisbatan ancha tezroq amalga oshirilishi mumkinligi ko‘rsatilgan. Taklif etilgan BKIKYU usulida qidiruv jarayoni $l/2$ qadam bilan chegaralanadi va bu modulni qisqa vaqt ichida faktorlash imkonini beradi.

4.2-Teorema (RSA modulida $\varphi(N)$ va N o‘rtasidagi kvadrat ildizlar yaqinligi). Berilgan RSA moduli $N = p \cdot q$, bu yerda p va q - o‘zaro turli tub sonlar, $p > q$ bo‘lganda, $\sqrt{N} - 2 < \sqrt{\varphi(N)} < \sqrt{N} - 1$, butun qism jihatidan $\left\lfloor\sqrt{\varphi(N)}\right\rfloor = \left\lfloor\sqrt{N}\right\rfloor - 1$ yoki $\left\lfloor\sqrt{\varphi(N)}\right\rfloor = \left\lfloor\sqrt{N}\right\rfloor - 2$, yaqinlik munosabati o‘rinli bo‘ladi.

Ushbu matematik asosga ko‘ra Butun kvadrat ildizlar kvadratining yaqinlashishi usuli (BKIKYU) usuli taklif qilindi. BKIKYU usulining maxfiy kalitni izlash bosqichlari quyida keltirilgan.

1-bosqich. Dastlabki qiymatlar tayyorlanadi. Berilgan N son uchun quyidagilar hisoblanadi:

$$r = \lfloor\sqrt{N}\rfloor^2, r_p = \lfloor\sqrt{N} - 1\rfloor^2$$

Bu qiymatlar N ga yaqin bo‘lgan ikkita kvadrat son sifatida olinadi.

2-bosqich. $\varphi(N)$ ning taxminiy qiymatini aniqlash. Har bir iteratsiyada o‘rtacha qiymat:

$$t = \sqrt{r \cdot r_p}$$

hisoblanadi. Ushbu t qiymati $\varphi(N)$ ning yaqinlashuvchi bahosi sifatida olinadi.

3-bosqich. Diskriminantni hisoblash. Taxminiy φ(N) asosida:

$$s = N - \varphi(N) + 1, D = s^2 - 4N$$

qiymatlar topiladi.

4-bosqich. Diskriminant holatini tahlil qilish. Agar $D < 0$, diskriminant manfiy bo‘lsa, bu holda haqiqiy ildiz mavjud emas; yuqori chegara t bilan almashtiriladi va $\left|r - r_p\right| \leq 2$ shart bajarilmagan bo‘lsa 2-bosqichga qaytiladi aks holda 5-bosqichga o‘tiladi. Agar $D \geq 0$, diskriminantning kvadrat ildizi olinadi: $\sqrt{D}$ va undan quyidagicha p hamda q qiymatlar aniqlanadi:

$$p = \frac{s + \left\lfloor\sqrt{D}\right\rfloor}{2}, q = s - p$$

Agar $p \cdot q = N$ sharti bajarilsa, jarayon yakunlanadi. Aks holda kichik chegara qiymati t bilan almashtiriladi va $\left|r - r_p\right| \leq 2$ shart bajarilmagan bo‘lsa 2-bosqichga qaytiladi.

5-bosqich. Usul yakunida oxirgi hisoblangan t qiymati qaytariladi. Yakuniy $\varphi(N)$ qiymati quyidagi oraliqdan qidiriladi:

$$\varphi(N) \in \{t - 1, t, t + 1\}$$

Ushbu usul yordamida:

- φ(N) ning yaqin qiymati topiladi;
- shundan so‘ng p va q aniqlanadi;
- natijada RSA algoritmining maxfiy kaliti $d = e^{-1} \bmod \varphi(N)$ hisoblanishi mumkin bo‘ladi.

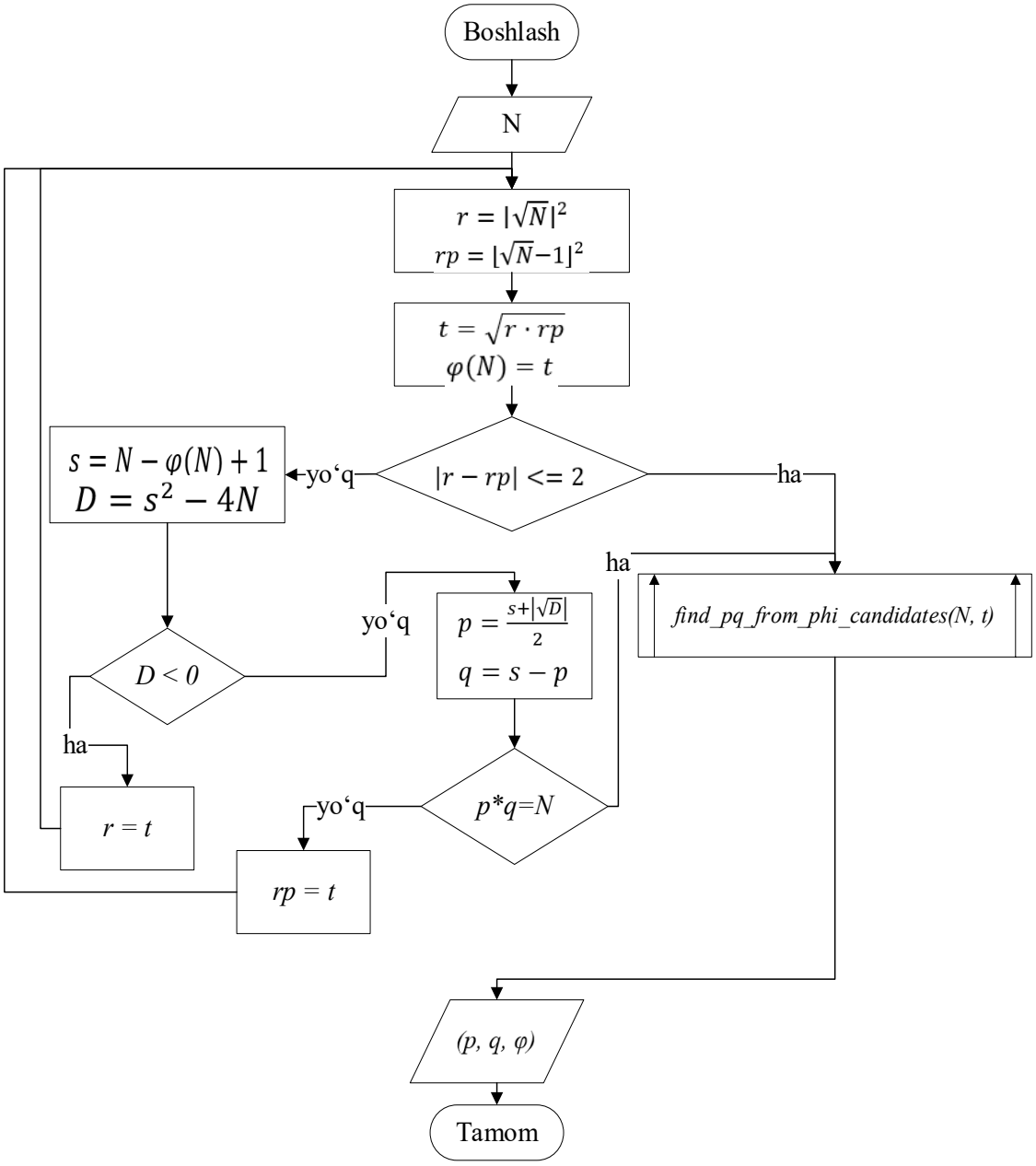
Ushbu usulning samaradorligi p va q qiymatlarining bir-biriga nisbatan yaqin bo‘lgan holatlarida yuqori bo‘ladi. Agar $p \approx q$ bo‘lsa, $\varphi(N)$ qiymati N ga nisbatan kvadrat ildiz yaqinlashuvi orqali tezda aniqlanadi.

Bobning uchinchi paragrafi “Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitlarini aniqlashning BKIKYU

algoritmi” deb nomlangan. 4.1-bo‘limda keltirilgan BKIKYU usuli asosida Butun kvadrat ildizlar yaqinlashishi usuli (BKIKYU) algoritmi ham ishlab chiqildi. Ishlab chiqilgan BKIKYU algoritmining asosiy maqsadi – RSA moduli bo‘lgan $N = p \cdot q$ sonini uning tub bo‘luvchilari p va q ga ajratishdir. Algoritm ikkita qism algoritmga ajratiladi. Dastlab *BKIKYU(N)* algoritmi $\varphi(N)$ (Eyler funksiyasi) ning taxminiy qiymatini topishga, keyingi *find_pq_from_phi_candidates(N, t)* algoritmi esa shu qiymat asosida p va q ni aniqlashga asoslangan (2-rasm).

Butun kvadrat ildizlar kvadratlarining yaqinlashish usuli va algoritmini ishlab chiqishda quyidagi teorema o‘rnatildi va isbotlandi.

4.3-Teorema. Faraz qilaylik $N = pq$ - ikki toq tub sonlarning ko‘paytmasi va $l - N$ ning bit uzunligi (ya’ni $2^{l-1} \leq N < 2^l$). Agar $|p - q| \leq 2^{[I/4]}$, bo‘lsa, u holda $\varphi(N) = N - 1 - 2 * \lfloor\sqrt{N}\rfloor$, ya’ni, $m = \lfloor\sqrt{N}\rfloor$ deb belgilansa $\varphi(N) = N - 1 - 2m$ o‘rinli.



2-rasm. BKIKYU algoritmining blok sxemasi

Ferma, Pollard va Shanks kabi usullar kichik va o‘rta bit uzunlikdagi sonlarda samarali bo‘lsa-da, bit uzunligi ortishi bilan hisoblash murakkabligi keskin oshadi. Raqamli dala elaklari (NFS) algoritmi hozirda eng kuchli umumiy usul sifatida tan olingan va yirik RSA sonlarini faktorizatsiya qilishda qo‘llaniladi. Taklif qilingan intervallarga bo‘lish algoritmi esa $|p - q| \leq 2^{l/4}$ shart bajarilganda bit uzunligidan qat’i nazar tezkor natija beradi va qisqa vaqt ichida $\varphi(N), p, q$ qiymatlarini aniqlash imkonini beradi. Bu jihati uni boshqa algoritmlardan ustun qo‘yadi.

4095 va 4096 bit uzunlikdagi modul sonlar ustida o‘tkazilgan tajribalar taklif qilingan algoritmning samaradorligini aniq namoyon qildi. Xususan, 4095 bitli N soni uchun algoritm $\varphi(N)$, qiymatlarini hisoblashni 0.000248 soniyada, 4096 bitli N soni uchun esa 0.000255 soniyada yakunladi. Ushbu natijalar taklif qilingan yondashuvning hisoblash tezligi tubdan yuqori ekanligini ko‘rsatadi: faktorizatsiya jarayoni butun sonlar kvadrat ildizini hisoblash va diskriminant tekshiruvlari kabi bir nechta oddiy arifmetik amallarga asoslanganligi sababli, juda qisqa vaqt oralig‘ida yakunlanmoqda.

Dissertatsiyaning beshinchi bobi “Ishlab chiqilgan usullar va algoritmlarning samaradorligini baholash natijalari” deb nomlangan. Mazkur bobda tadqiqot davomida taklif etilgan usullar va algoritmlarning samadorligini baholash, jumladan, BBKS usulining mavjud umumiy kritpografik talablar bilan o‘zaro ta’siri hamda akslantirishlarning kriptotahlil usullariga bardoshligiga ta’siri nuqtai nazaridan, faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarini baholash uchun ishlab chiqilgan KATAOF, MOKM, BKIKYU usullari va ular asosida ishlab chiqilgan algoritmlarning boshqa shu turdagi algoritmlar bilan qiyosiy solishtirish, ya’ni hisoblash murakkabligi nuqtai nazaridan baholash amalga oshirilgan.

Bobning birinchi paragrafi “BBKS usulining chiziqsiz akslantirishlar bardoshligiga ta’siri” deb nomlangan. Tahlilga ko‘ra, 4×4 o‘lchamli S-boxlarda BBKS xarakteristikasi eng avvalo strukturaviy xossalarga, xususan fiksatsiyalangan nuqtalar (FP) va qarama-qarshi fiksatsiyalangan nuqtalar (OFP) mavjudligiga qisman sezilarli darajada bog‘liq ekanligi kuzatiladi. Magma S-boxlarida FP va OFP qiymatlari mavjud bo‘lgan hollarda BBKS chetlanishlar soni 1–5 oralig‘ida bo‘lib, bu taqsimot muvozanati buzilganini ko‘rsatadi. Aksincha, FP=0 va OFP=0 bo‘lgan S-Box1–S-Box5 va S-Box9–S-Box20 guruhlarida BBKS chetlanishlari 0 ga teng, ya’ni 2-bitli kirish–chiqish juftliklari bir tekis taqsimlangan.

Shuningdek, BBKS ko‘rsatkichi qat’iy lavin effekti xossasi (SAC) bilan o‘rtacha darajada bog‘liq ekanligi aniqlandi. SAC qiymati 0.5 ga yaqinlashgan sari BBKS chetlanishlari sonining ko‘payishini ko‘rsatadi, SAC ≈ 0.625–0.656 bo‘lgan S-boxlarda esa BBKS optimal holatga yaqinlashadi. Biroq, barcha S-boxlarda chiziqsizlik (NL=4), korrelyatsiya immuniteti (CI=0) va algebraik daraja (AI=2) bir xil bo‘lgani sababli, BBKS bu ko‘rsatkichlarga bevosita bog‘liq emas degan xulosa chiqarish mumkin. Demak, BBKS asosan lokal strukturaviy simmetriya va differensial muvozanat bilan belgilanadi, umumiy chiziqsizlik ko‘rsatkichlari bilan esa to‘g‘ridan-to‘g‘ri bog‘lanmagan. Tahlil natijalari 8-jadvalda keltirilgan.

8-jadval.

4×4 o‘lchamli S-box jadvallarining umumiy kriptografik talablarga baholash natijalari va BBKS xarakteristikasi

S-box	B	SAC (=0.5)	FP	OFP	Big_SAC (=0.5)	NL	CI	AI	BBKS (Chetlanishlar (Soni))
Magma_1	+	0.5156	1	0	0.520	4	0	2	1/3 (5)
Magma_2	+	0.5469	4	1	0.510	4	0	2	1/3 (2)
Magma_3	+	0.5156	1	0	0.541	4	0	2	1/3 (1)
Magma_4	+	0.5312	2	2	0.541	4	0	2	1/3 (3)
Magma_5	+	0.5625	2	0	0.510	4	0	2	1/3 (0)
Magma_6	+	0.5459	1	1	0.552	4	0	2	1/3 (3)
Magma_7	+	0.5938	1	1	0.531	4	0	2	1/3 (1)
Magma_8	+	0.5	2	0	0.562	4	0	2	1/3 (4)
Present	+	0.625	0	1	0.562	4	0	2	1/3 (0)
S-Box1	+	0.500	0	0	0.500	4	0	2	1/3 (2)
S-Box2	+	0.500	0	0	0.500	4	0	2	1/3 (4)
S-Box3	+	0.500	0	0	0.500	4	0	2	1/3 (3)
S-Box4	+	0.500	0	0	0.500	4	0	2	1/3 (4)
S-Box5	+	0.640	0	0	0.541	4	0	2	1/3 (0)
S-Box6	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box7	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box8	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box9	+	0.640	0	0	0.552	4	0	2	1/3 (0)
S-Box10	+	0.656	0	0	0.520	4	0	2	1/3 (0)
S-Box11	+	0.640	0	0	0.541	4	0	2	1/3 (0)
S-Box12	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box13	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box14	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box15	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box16	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box17	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box18	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box19	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box20	+	0.625	0	0	0.562	4	0	2	1/3 (0)

Bobning ikkinchi paragrafi “KATAOF usulining hisoblash murakkabligi” deb nomlangan. Ushbu paragrafda KATATOF usulining hisoblash murakkabligi $O((\log N)^2)$ ga tengligi ko‘rsatilgan.

Bobning uchinchi paragrafi “MOKM usulining hisoblash murakkabligi” deb nomlangan. Ushbu paragrafda MOKM usulining hisoblash murakkabligi $O((\log N)^3)$ ga tengligi ko‘rsatilgan.

Bobning to‘rtinchi paragrafi “BKIKYU usulining hisoblash murakkabligi” deb nomlangan. Ushbu paragrafda BKIKYU usulining hisoblash

murakkabligi $|p-q| \le 2^{\frac{l}{4}}$ da $O(l/2)$ va $|p-q| > 2^{\frac{l}{4}}$ da $O\left(2^{l/2} \cdot l\right)$ ga tengligi aniqlandi.

Faktorizatsiyalash algoritmlarining hisoblash murakkabligi bo‘yicha qiyosiy tahlili 9-jadvalda keltirilgan.

9-jadval.

Faktorizatsiyalash algoritmlarining qiyosiy tahlili

Usul yoki algoritm nomi	Asosi	Effiktiv chegarasi	Hisoblash murakkabligi	Izoh
Fermaning faktorizatsiya usuli	$N = x^2 - y^2$ ko‘rinishida ifodalash	Umumiy holda ~130–150 bit	$O\left(N^{1/2}\right)$ eng yaxshi holatda $O\left(N^{1/4}\right)$	Faqat yaqin omillarga mos
Pollardning ρ algoritmi	Tug‘ilgan kun paradoksi	130–200 bit sonlargacha samarali	$O(N^{1/4})$	Eng samarali probabilistik kichik tub bo‘luvchilar uchun
Pollard–Strassen algoritmi	ρ + FFT kombinatsiyasi	~150–200 bit	$O(N^{\frac{1}{4}} * log_4 N)$	Katta sonlarda samaradorligi cheklangan.
Shanksning kvadratik shakl usuli (SQUFOF)	Kvadratik shakllar orqali yaqin ildizlarni izlash	~100 raqam (≈ 330 bit) sonlargacha yaxshi	$O(N^{\frac{1}{4}+\varepsilon})$	O‘rtacha kattalikdagi sonlarda samarali.
Pollardning p−1 algoritmi	p−1 kichik omillarga bo‘linadigan bo‘lsa	p−1 kichik omillarga bo‘linadigan bo‘lsa	$O(N^{\frac{1}{4}} * log^c N)$	Maxsus tub bo‘luvchilar uchun tez
Leman algoritmi	kvadrat ildiz qidiruvi	70–85 bit sonlargacha	$O(N^{1/3})$	amalda o‘rnini QS bosgan
Dixon algoritmi	Kvadrat kongruensiya yig‘ish	~100 raqam (≈ 330 bit) sonlargacha	$L_N(\frac{1}{2}, 2\sqrt{2})$	QS’ning oldingi bosqichi
Davomli kasrlar usuli (CFRAC)	Kasr yaqinlashuvlaridan foydalanish	~110–120 raqam (≈ 360–400 bit) sonlargacha	$L_N(\frac{1}{2}, 2\sqrt{2})$	QS’ga o‘rin bo‘shatgan
Kvadrat g‘alvir (QS/MPQS)	Ferma usulining umumlashgan shakli	~120–130 raqam (≈ 400–430 bit) sonlargacha	$L_N(\frac{1}{2}, 1)$	GNFS paydo bo‘lgunga qadar eng tezkor umumiy usul
Lenstra ECM (Elliptic Curve Method)	Elliptik egri chiziqlar maxsus faktorizatsiya	200–400 bitli tub omillarni samarali ajratadi	$L_p(\frac{1}{2}, 2\sqrt{2})$, p – eng kichik tub bo‘luvchi	Kichik/orta tub bo‘luvchilar uchun eng yaxshi
NFS usuli	Algebraik/sonli maydonlarda g‘alvirlash	200 raqam (≈ 660 bit)	$L_N(\frac{1}{3}, \sqrt[3]{\frac{64}{9}})$	Hozirgi kunda eng tezkor umumiy algoritm
KATAOF	Tom-Kuk ko‘paytirish usuli	Mumkin bo‘lgan amaliy xotira	$O((\log N)^2)$	4 bitli qismlarga ajratib faktorlashda 16! xotira zarur
MOKM	Intervallarga tegishliligini taxmin qilishga asoslangan	Intervallarni muvaffaqiyatli taxminiga bog‘liq	$\begin{cases} O((\log N)^3) \\ O(N \cdot (\log N)^3) \end{cases}$	Intervallarni muvaffaqiyatli taxminlarida samarali
BKIKYU	$[\sqrt{N} - 1^2, \sqrt{N}]$ intervalni teng bo‘lib borishga asoslangan	$\lvert p-q \rvert \le 2^{l/4}$ shart bajarilsa bit uzunligi cheklanmagan	$O(l/2), \lvert p-q \rvert \le 2^{\frac{l}{4}}$ $O\left(2^{l/2} \cdot l\right), \lvert p-q \rvert >$	$\lvert p-q \rvert \le 2^{\ell/4}$ shart bajarilmasa algoritmning xatoligi $p + q - 2 * \sqrt{N} \pm 2$

UMUMIY XULOSALAR

Dissertatsiya ishida qo‘yilgan maqsad va vazifalardan kelib chiqib quyidagi natijalar olindi:

1. Simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholashning “Bitlarning birgalikda kelishlari soni” deb nomlangan yangi usuli ishlab chiqilgan, mazkur usul S-box akslantirishlarini baholashda mavjud umumiy kriptografik talablarga qo‘shimcha talab sifatida xizmat qiladi va chiziqsiz akslantirishlarga kirish bitlarining birgalikda kelishlari chiqishda qanday tartibda takrorlanishiga asoslangan holda shifrlash kalitlarini aniqlash imkonini bergan;

2. Simmetrik shifrlash algoritmlarinining chiziqsiz akslantirishlarini baholashning “Bitlarning birgalikda kelishlari soni” deb nomlangan yangi usuli asosida shifrlash kalitini aniqlashning ikkita algoritmi ishlab chiqilgan, mazkur algoritmlar 4x4 o‘lchamli S-box akslantirishlariga mos maxfiy kalitning 75 foizini, ayrim S-boxlar uchun esa 100 foiz aniqlik bilan taxmin qilish imkonini berdi;

3. Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan yangi ko‘paytirish amallariga teskari amallar orqali faktorlash (KATAOF) usuli ishlab chiqilgan, mazkur usul sonlarni ko‘paytirishdagi munosabatlar orqali faktorlash imkonini beradi;

4. Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun sonlarni ko‘paytirishning Tom-Kuk usuliga asoslangan KATAOF usuli asosida ikkita KATAOF-1 va KATAOF-2 faktorlash algoritmlari ishlab chiqilgan, mazkur algoritmlar $2^{\frac{l}{2}-2}$ xotirani ta’minlash imkoniyati mavjud bo‘lganda l bitli RSA ochiq kalitli shifrlash algoritmining modulini faktorlash imkonini beradi;

5. Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlarining maxfiy kalitni aniqlashning maxfiy va ochiq kalitlar munosabatiga asoslangan kichik razryadli RSA modullarida samarali hisoblangan MOKM usuli ishlab chiqilgan, mazkur usul p va q tub sonlarning qaysi intervallarga tegishli bo‘lishi mumkinligining muvaffaqiyatli taxminlarida maxfiy kalitni aniqlash imkonini beradi;

6. Faktorlash muammosiga asoslangan ochiq kalitli shifrlash algoritmlari uchun maxfiy kalitlarni aniqlashning butun kavdrat ildizlar kavadratining yaqinlashuvi usuli (BKIKYU) deb nomlangan maxfiy kalitlarni aniqlash usuli ishlab chiqilgan, mazkur usul asosida algoritm ishlab chiqilgan, mazkur algoritm RSA ochiq kalitli shifrlash algoritmining moduli l bit bo‘lganda, $|p-q| \le 2^{\frac{l}{4}}$ shart bajarilganda $\frac{l}{2}$ qadam bilan maxfiy kalitlarni aniqlash imkonini berdi.

НАУЧНЫЙ СОВЕТ DSc.03/2025.27.12.FM.01.03
ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ ПРИ
НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

БОЙКУЗИЕВ ИЛХОМ МАРДАНОКУЛОВИЧ

МЕТОДЫ И АЛГОРИТМЫ ОЦЕНКИ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ И АЛГОРИТМОВ ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ

05.01.05 – Методы и системы защиты информации. Информационная и кибербезопасность

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА НАУК (DSc)
ПО ФИЗИКО-МАТЕМАТИЧЕСКИМ НАУКАМ

Ташкент – 2026

Тема диссертации доктора наук (DSc) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за B2026.DSc/FM316.

Диссертация выполнена в Национальном Университете Узбекистана имени Мирзо Улугбека.

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

Научный советник:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
Официальные оппоненты:	**Курьязов Давлатяр Матякубович** доктор физико-математических наук
	Туйчиев Гулям Нумонович доктор физико-математических наук
	Ботиров Файзулладжан Бахтиярович доктор технических наук, доцент
Ведущая организация:	**Военный институт информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан**

Защита диссертации состоится «_____» _____ 2026 года в _____ часов на заседании Научного совета DSc.03/2025.27.12.FM.01.03 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-72-24, факс: (+99871) 246-53 -21, e-mail: nauka@nuu.uz).

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

Автореферат диссертации разослан «_____» _____ 2026 года
(протокол рассылки №____ от «_____» _____ 2026 года).

М.М. Арипов
Председатель Научного совета по-присуждению ученых степеней, доктор физико-математических наук, профессор

З.Р. Рахмонов
Ученый секретарь Научного совета по-присуждению ученых степеней, доктор физико-математических наук, доцент

А.В. Кабулов
Председатель Научного семинара при научном совете по присуждению учёных степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация докторской диссертации (DSc))

Актуальность и востребованность темы диссертации. Во всем мире особое внимание уделяется вопросам оценки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом к методам криптоанализа, в частности разработке методов и алгоритмов, оценки устойчивости нелинейных преобразований к криптоаналитическим атакам, направленных на прогнозирование (угадывание) или определение значений ключей шифрования и определение секретных ключей алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, а также на факторизацию достаточно большого модуля в алгоритмах шифрования с открытым ключом. В действующих криптографических системах используемые алгоритмы, длины ключей и параметры должны регулярно пересматриваться с учётом современных методов криптоанализа и вычислительных возможностей аппаратных средств. По данным Chainalysis, «в 2024 году ущерб, причинённый атаками на криптографические системы во всем мире, увеличился на 21,07% по сравнению с 2023 годом и составил 2,2 миллиарда долларов США» [4]. Для предотвращения ущерба такого масштаба необходимо оценивать безопасность криптосистем на основе многоуровневого комплексного подхода, в том числе с применением методов оценки, опирающихся на вычислительную сложность математических задач. В связи с этим особое внимание уделяется задачам, связанным с разработкой современных методов криптоанализа для оценки симметричных и асимметричных алгоритмов шифрования.

В мире ведутсямасштабные научные исследования, направленные на разработку стойких криптографических алгоритмов и повышение их надёжности в целях обеспечения информационной безопасности. В этих исследованиях, прежде всего, в качестве актуальной задачи рассматриваются выявление слабых мест действующих алгоритмов шифрования с использованием методов криптоанализа, оценка их устойчивости к различным моделям атак, а также проектирование безопасных и надёжных алгоритмов на основе полученных результатов. Важное значение имеет оценка криптографической стойкости нелинейных преобразований, применяемых в алгоритмах симметричного шифрования, на основе математических критериев. В целях обеспечения устойчивости к дифференциальному, линейному, алгебраическому и иным методам криптоанализа особое внимание уделяется анализу свойств S-блоков и других нелинейных компонентов, а в криптографии с открытым ключом исследования сосредоточены на углубленном изучении математических основ систем шифрования, оценке их степени сложности, а также разработке методов оценки, основанных на новых подходах, обеспечивающих их устойчивость к существующим и потенциальным атакам.

В нашей республике большое внимание уделяется обеспечению информационной безопасности, в частности развитию области криптологии, организации криптографической защиты информации, разработке стойких криптографических алгоритмов и созданию современных методов криптоанализа. В частности, в последние годы достигаются определенные

[4] https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

результаты в реформах, проводимых в сфере образования и развития науки в области криптологии. В Постановлении Президента Республики Узбекистан № ПП-293 «О дополнительных мерах по развитию образования и науки в сфере криптологии в Республике Узбекистан» подчёркивается необходимость непрерывного совершенствования криптографических алгоритмов, применяемых для защиты информации и в программе научно-исследовательских работ по актуальным направлениям развития национальной криптологии Республики Узбекистан на 2024–2028 годы, утверждённой данным постановлением, предусмотрено выполнение научно-исследовательской работы по разработке современных методов криптоанализа[2]. В процессе реализации указанных задач важное значение имеют разработка новых методов оценки и анализа криптостойкости современных криптографических алгоритмов, проведение экспериментальных исследований по оценке сложности криптографических алгоритмов на основе разработанных методов, а также оценка эффективности этих методов.

Настоящее диссертационное исследование в определённой степени способствует реализации задач, установленных Законом Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности», Указом Президента Республики Узбекистан от 28 января 2022 года № ПФ-60 «О Стратегии развития Нового Узбекистана на 2022–2026 годы», постановлением Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан», постановлением Президента Республики Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критически важной информационной инфраструктуры Республики Узбекистан», а также иными нормативно-правовыми актами, относящимися к данной сфере деятельности.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в рамках приоритетного направления развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий».

Обзор научных исследований по теме диссертации.

Научные исследования в области криптографических методов защиты информации, создании симметричных алгоритмов шифрования и их оценки методами криптоанализа, создании симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом, а также оценки их криптостойкости проводятся ведущими мировыми научно-исследовательскими центрами и высшими учебными заведениями, включая: Национальный институт стандартов и технологий (NIST, США), Агентство национальной безопасности (NSA, США), Европейский институт телекоммуникационных стандартов (ETSI, Франция), Международную организацию по стандартизации (ISO, Швейцария), Институт инженеров по электротехнике и электронике (IEEE, США), ООО «UNICON.UZ» (Узбекистан), Массачусетский технологический институт

[2] O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” gi PQ-293 sonli Qarori

(США), Стэнфордский университет (США), Калифорнийский университет (США), Университет Карнеги - Меллона (США), Оксфордский университет (Великобритания), Кембриджский университет (Великобритания), Федеральный технологический институт Цюриха (Швейцария), Федеральную политехническую школу Лозанны (Швейцария), Мюнхенский технический университет (Германия), Католический университет Лёвена (Бельгия), Национальный университет Сингапура (Сингапур), Университет Цинхуа (Китай), Пекинский университет (Китай), Токийский университет (Япония), Корейский институт передовых наук и технологий (KAIST, Республика Корея), Тель-Авивский университет (Израиль), Институт науки Вейцмана (Израиль), Индийский технологический институт (Индия), Наньянский технологический университет (Сингапур), Российскую академию наук (Россия), Московский государственный университет (Россия), Санкт-Петербургский государственный университет (Россия), Белорусский государственный университет (Беларусь), Национальный университет Казахстана (Казахстан), Кыргызско-Турецкий университет Манас (Кыргызстан), Национальный университет Таджикистана (Таджикистан), Национальную академию наук Азербайджана (Азербайджан), Ташкентский университет информационных технологий имени Мухаммада ал-Хорезмий (Узбекистан), Центр цифровых технологий и информационных технологий при Ташкентском университете информационных технологий имени Мухаммада ал-Хорезмий (Узбекистан) и Национальный университет Узбекистана имени Мирзо Улугбека (Узбекистан).

В результате исследований, проведённых в мире в области криптографических методов защиты информации, создании симметричных алгоритмов шифрования и их оценки методами криптоанализа, создании симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом, а также оценки их криптостойкости, получены следующие результаты: разработаны новые конструкции симметричных алгоритмов шифрования на основе их S-блоков и нелинейных преобразований; выполнена математически обоснованная проверка их безопасности; получены и доказаны теоретические и практические результаты по криптографической оценке алгоритмов шифрования с открытым ключом и их применению в прикладных системах.

Например, в научных центрах и университетах России и США проводились исследования по выявлению слабых мест симметричных алгоритмов шифрования на основе их анализа и по их оптимизации; в университетах США, Китая и Японии изучались алгоритмы постквантовой криптографии и методы криптоанализа, в исследовательских центрах Германии, США и Швейцарии в области шифрования с открытым ключом и алгоритмов электронной цифровой подписи разрабатывались математические модели, оценивались длины ключей и параметры безопасности; в университетах Франции и Италии выполнялись разработки по тестированию электронной цифровой подписи и криптографических протоколов в прикладных системах. В научных центрах Республики Корея, Израиля, США, России и Индии в рамках развития методов криптоанализа были разработаны подходы к алгебраическим атакам, дифференциальному и линейному анализу, а также механизмы защиты от атак по побочным каналам. Масштабные научные исследования по симметричным

алгоритмам шифрования и алгоритмам шифрования с открытым ключом и оценке их криптостойкости проводились в Институте математики им. С. Л. Соболева Российской академии наук, Институте вычислительной математики и математической геофизики, Институте вычислительной математики Уфимского научного центра, а также в Московском и Санкт-Петербургском государственных университетах.

Исследования в данной области ведутся в университетах и научных центрах США, Великобритании, России, Швейцарии, Германии, Италии, Китая, Японии и Республики Корея, а также в Республике Узбекистан - в Ташкентском университете информационных технологий имени Мухаммада ал-Хорезмий, ООО «UNICON.UZ», Центре цифровых технологий и информационных технологий при Ташкентском университете информационных технологий имени Мухаммада ал-Хорезмий и Национальном университете Узбекистана имени Мирзо Улугбека.

В мире продолжаются научные исследования, посвящённые методам и алгоритмам оценки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом. В рамках этих исследований изучаются приоритетные направления, включая: оценка симметричных алгоритмов шифрования к методам криптоанализа и создание их нелинейных преобразований в соответствии с общими криптографическими требованиями и применение новых подходов в процессе оценки, разработка новых методов оценки алгоритмов с открытым ключом, в том числе создание методов и алгоритмов для определения секретных ключей и параметров в криптосистемах, основанных на проблеме факторизации, посредством анализа соотношений между открытым и секретным ключами; а также разработкановых методов и алгоритмов факторизации с применением современных подходов.

Степень изученности проблемы. В области криптографической защиты информации, разработки симметричных алгоритмов шифрования и оценки их стойкости к методам криптоанализа исследования проводились такими учёными, как H. Feistel, M. Matsui, J. Daeman, D. Knut, S. Maitra, A. Youssef, N. Tokereva, O. Rothaus, X. Zhang, A. Webster, Y. Liu, L. Brown, V. Parihar, A. Sorkin, X. Zhu, A. Biryukov, M. Dawson, S. Fischer, K. Zamli, N. Siddiqui, M. Spain, C. Carlet, W. Meiyer, W. Stallings, C. Pomerance, J. Ding, M. Kavut, I. Yilmaz, T. Kasami, S. Tavares, Y. Yang, W. Zang, Y. Wang, M. Ahmad, L. Babenko, E. Ishukova, E. Maro, кроме того, разработки алгоритмов шифрования с открытым ключом на основе задач различной вычислительной сложности и методов их оценки исследования выполнялись такими учёными, R. Rivest, A. Shamir, L. Adleman, N. Koblitz, M. Pollard, A. Lenstra, R. Leman, J. Dixon, A. Joux, K. Lauter, M. Morrison, C. Pomerance, P. Montgomery и др.

В нашей республике исследования в области криптографических методов защиты информации, хеш-функций, разработки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом, алгоритмов электронной цифровой подписи, а также оценки их криптостойкости проводились такими исследователями, как П. Хасанов, М. Арипов, М. Каримов, С. Ганиев, Б. Абдурахимов, А. Кабулов, Д. Акбаров, Х. Хасанов, О. Ахмедова, Г. Жураев, Д. Курьязов, Г. Тучиев, Б. Ахмедов, А. Сатторов, З. Худойкулов. О.

Алланов, М. Бердыморудов, У. Мардиев.

Вопросы оценки с использованием методов криптоанализа рассмотрены в научных работах ряда ученых, в частности А. Бирюкова, N. Courtois, M. Matsui, M. Pollard, A. Lenstra, R. Leman, J. Dixon, A. Joux, Л. Бабенко, М. Арипова, Б. Абдурахимова, Г. Жораева, Д. Курязова, А. Саттарова, М. Бердимуродова и др.

Вместе с тем вопросам оценки нелинейных преобразований симметричных поточных шифров, применения современных технологий при определении ключей шифрования, а также разработке новых подходов к определению секретных ключей в алгоритмах шифрования с открытым ключом уделено недостаточное внимание.

Связь диссертационного исследования с планами научно-исследовательских работ учреждения, в котором выполнена диссертация. Диссертационное исследование выполнено фундаментального проекта Национальный университет Узбекистана имени Мирзо Улугбека F-OT-2021-248 «Разработка интеллектуальных методов и технологий выявления, идентификации и устранения угроз для защиты информации на основе функциональных таблиц», а также в рамках прикладного научно-исследовательского проекта Национального университета Узбекистана имени Мирзо Улугбека № AL-9624115223 - «Создание электронного учебника по криптографии».

Цель исследования является разработка решений на основе новых подходов к оценке безопасности симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом.

Задачи исследования:

разработка нового метода оценки нелинейных преобразований симметричных алгоритмов шифрования;

разработка алгоритма на основе нового метода оценки нелинейных преобразований симметричных алгоритмов шифрования;

разработка нового метода факторизации для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации;

разработка алгоритма на основе нового метода факторизации для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации;

разработка метода определения секретных ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации;

разработка нового метода определения секретных ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, а также разработка алгоритма на основе данного метода.

В качестве **объекта исследования** выбраны симметричные алгоритмы шифрования и алгоритмы шифрования с открытым ключом.

Предмет исследования составляют методы оценки криптостойкости симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом.

Методы исследования. В ходе исследования использовались методы прикладной криптографии и криптоанализа, теории чисел, теории вероятностей, сравнительного анализа, а также методы проведения экспериментов на основе

объектно-ориентированного программирования.

Научная новизна исследования заключается в следующих:

разработан метод оценки нелинейных преобразований симметричных алгоритмов шифрования, позволяющий определять ключи шифрования на основе порядка повторений совместных появлений входных битов на выходе нелинейных преобразований и служащий дополнительным требованием к существующим общим криптографическим критериям при оценке S-box- преобразований;

разработаны алгоритмы определения ключа шифрования на основе метода оценки нелинейных преобразований симметричных алгоритмов шифрования, которые позволяют оценить секретный ключ с точностью до 75%, соответствующего S-box-преобразованиям размерности 4×4 и со 100% точностью для некоторых S-box;

разработан метод факторизация посредством обратных операций к умножению, основанный на методе умножения Тоома-Кука позволяющий факторизацию на основе соотношений, возникающих при умножении чисел;

разработаны новые алгоритмы факторизации, основанные на методе, разработанном на основе метода умножения Тоома-Кука позволяющий факторизации модуля l-битного RSA-алгоритма шифрования с открытым ключом при наличии достаточного объёма памяти порядка $2^{\frac{l}{2}-2}$;

разработан эффективный метод определения секретного ключа в малобитных модулях RSA, учитывающий соотношения секретного и открытого ключей для алгоритмов шифрования с открытым ключом основанный на проблемы факторизации, данный метод позволяет определить секретный ключ при успешном прогнозировании того, к каким интервалам могут принадлежать простые числа p и q;

разработан метод определения секретных ключей, для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, который позволяет обнаруживать секретные ключи с шагом $\frac{l}{2}$ при условии $|p-q| \leq 2^{\frac{l}{4}}$ в l -битном модуле алгоритма шифрования с открытым ключом *RSA,* на основе данного метода разработан алгоритм.

Практические результаты исследования заключаются в следующих:

разработано программное средство, реализующее алгоритм оценки, разработанный на основе нового метода «число совместных появлений битов» для анализа нелинейных преобразований симметричных алгоритмов шифрования;

разработано программное средство, реализующее алгоритм факторизации на основе нового метода факторизации, построенного на методе умножения чисел Тоома-Кука, для алгоритмов шифрования с открытым ключом, основанных на проблеме;

разработан алгоритм для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, на основе метода определения секретных ключей, построенного на разбиении на интервалы.

Достоверность результатов исследования. Достоверность результатов, полученных в диссертации, обусловлена строгостью приведённых математических рассуждений, подтверждением на основе результатов проведённых численных исследований, а также реальными и

экспериментальными данными, полученными при применении разработанных новых методов и алгоритмов к алгоритмам шифрования.

Научная значимость результатов исследования. Научная значимость результатов исследования определяется тем, что разработанный метод оценки нелинейных преобразований может быть использован при проектировании преобразований данного типа, а также при генерации параметров секретного ключа в алгоритмах, основанных на проблеме факторизации.

Практическая значимость результатов исследования. Практическая значимость результатов исследования обусловлена тем, что разработанные программные средства, реализующие предложенные методы и алгоритмы, могут быть использованы для оценки существующих алгоритмов шифрования с открытым ключом, а также для анализа нелинейных преобразований алгоритмов шифрования.

Внедрение результатов исследования. По результатам, полученным с использованием предложенных алгоритмов и разработанных на их основе программных средств:

метод оценки нелинейных преобразований симметричных алгоритмов шифрования, позволяющий определять ключи шифрования на основе порядка повторений совместных появлений входных битов на выходе нелинейных преобразований и служащий дополнительным требованием к существующим общим криптографическим критериям при оценке S-box- преобразований использован при анализе и оценке S-box симметричного алгоритма шифрования SM4 в рамках по естественным наукам № JSKY2021098 Цзининского педагогического университета Китайской Народной Республики под названием «Исследование алгоритма SM4» (справка Цзининского педагогического университета от 15.10.2025 № 20251015-001). В результате при оценке S-box преобразования алгоритма SM4 на основе свойства NCOB были выявлены отклонения (outlierlar), в частности установлено, что при значениях входных битов 0-го и 2-го разрядов (1,0) число совместных появлений выходных битов 0-го и 2-го разрядов со значениями (0,1) составляет 10, тогда как при тех же значениях входных битов (1,0) число совместных появлений выходных битов 0-го и 2-го разрядов со значениями (1,1) составляет 24. Полученные результаты позволили прогнозировать соответствующие биты ключа последнего раунда с точностью до 75%;

метод разработанный на основе метода умножения Том-Кука позволяющий факторизации модуля l -битного RSA-алгоритма шифрования с открытым ключом при наличии достаточного объёма памяти порядка $2^{\frac{l}{2}-2}$ был использован в зарубежных публикациях (Journal of Machine and Computing, 05(03), 2025, pp.1944-1957; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp.842-862; Symmetry, 16, 2024, ID 764) при проведении комплексного анализа эффективности алгоритма Шора с применением симулируемых квантовых бэкэндов (backend), предоставляемых платформой Qiskit. В результате была предложена гибкая и общая реализация факторизации целых чисел, которая позволяет динамически вводить факторизуемые числа, выбор случайных взаимно простых чисел, а также автоматически генерировать квантовые схемы;

метод оценки нелинейных преобразований симметричных алгоритмов

шифрования, основанный на анализе порядка повторения на выходе совместных комбинаций входных битов и позволяющий определять ключи шифрования, а также разработанные на его основе алгоритмы определения ключа шифрования были использованы в зарубежных публикациях (Discover Internet of Things, 5, 2025, pp.1-20; Multimedia Tools and Applications, 8, 2024, pp.24859–24886; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp.842-862) при создании быстродействующих и устойчивых систем безопасности для передачи данных, разработки рекомендаций по оптимальным требованиям и математической модели связи на основе параметров IoT и криптографических стандартов NIST, а также при развитии криптографических протоколов за счёт применения методов шифрования и дешифрования на основе теории графов. В результате было показано, что алгоритм, разработанный с использованием предложенного метода и алгоритмов, превосходит традиционный подход Trivium, время шифрования и дешифрования сокращается в соотношении 1:24, что делает его подходящим для быстрых требований к безопасности, также продемонстрирована возможность адаптации решений для лёгковесных IoT-инфраструктур, а применение графов декартова произведения и полных двудольных графов позволяет повысить конфиденциальность и целостность данных в системах связи;

метод оценки нелинейных преобразований симметричных алгоритмов шифрования, основанный на анализе порядка повторения на выходе совместных комбинаций входных битов и позволяющий определять ключи шифрования был использован в рамках проекта «Разработка облачного сервиса электронной цифровой подписи» при генерации параметров алгоритмов ЭЦП и оценке стойкости криптографических алгоритмов (справка ООО «UNICON.UZ», Центр научно-технических и маркетинговых исследований, от 29.01.2026 № 7-2/211). В результате метод разбиения на интервалы для определения секретных ключей для алгоритмов шифрования, основанных на проблеме факторизации, позволил систематически оценивать их при генерации криптографически стойких ключей, а новый метод оценки нелинейных преобразований симметричных алгоритмов шифрования, называемый «число совместных появлений битов» позволил оценить стойкость криптографических алгоритмов.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 16 научно-практических конференциях, в том числе на 4 международных и 12 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По теме диссертации опубликовано всего 43 научные работы, в том числе 20 статей - в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов диссертаций; из них 11 - в зарубежных изданиях (9 статей индексируются в базе Scopus), и 9 - опубликованы в республиканских журналах. Также, получены 7 свидетельств о регистрации программных средств для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка использованной литературы и приложений. Общий объём диссертации составляет 153 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснованы актуальность и необходимость проведённых исследований, а также их соответствие приоритетным направлениям развития науки и технологий республики. Приведены краткие сведения о зарубежных исследованиях по теме диссертации и степень изученности проблемы; определены цель и задачи исследования, объект и предмет; изложены научная новизна и практические результаты; раскрыта научная и практическая значимость полученных результатов; приведены сведения о внедрении результатов исследования в практику, опубликованных работах и структуре диссертации.

Первая глава диссертации озаглавлена **«Методы оценки современных криптографических алгоритмов»**; в ней выполнен всесторонний анализ методов оценки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом, составляющих ключевые направления современных криптографических систем. В ходе исследования изучены математические основы обеих разновидностей криптосистем, их критерии безопасности и методологии оценки, а также с научной точки зрения обобщены их преимущества и ограничения Первый параграф под названием **«Симметричные алгоритмы шифрования и методы оценки их нелинейных преобразований»** посвящён методам анализа нелинейных преобразований симметричных алгоритмов шифрования, в нём рассмотрены методы анализа нелинейных преобразований симметричных алгоритмов шифрования, в частности механизмы оценки по показателям степени линейности, алгебраической иммунности, устойчивости к дифференциальному и линейному криптоанализу, а также по критериям нелинейности S-box. Было установлено, что данные методы тесно связаны с внутренней структурой блочного алгоритма, числом раундов и длиной ключа; их взаимное влияние обосновано в математических терминах.

Второй параграф главы, озаглавлена **«Методы оценки алгоритмов шифрования с открытым ключом»**, в нём рассмотрены методы оценки безопасности алгоритмов шифрования с открытым ключом, а также проанализированы лежащие в их основе математические проблемы - факторизация, дискретное логарифмирование, а также эллиптических кривых. Особое внимание уделено изучению вычислительной сложности математических задач, лежащих в основе безопасности алгоритмов RSA, El-Gamal и ECC, а также современных алгоритмических подходов (Pollard rho, Quadratic Sieve, ECM, GNFS), влияющих на их решение. Также было отмечено, что с появлением моделей квантовых вычислений уровень безопасности этих алгоритмов пересматривается.

Поскольку некоторые базовые алгоритмы вычисления дискретного логарифма в конечных полях и определения порядка точки на эллиптической кривой прямо опирается на проблеме факторизации или принципах методов факторизации, представляется логичным рассматривать методы факторизации в качестве приоритетного направления. Метрики факторизации (smoothness, деревья subproduct, сложность в L-нотации) играют центральную роль при

оценке эффективности методов решения задачи порядка DLP и ЭК, поэтому углублённое изучение прежде всего алгоритмов факторизации (Pollard-rho, ECM, QS, NFS и др.) является эквивалентным либо даже более значимым этапом. Поэтому в этом разделе подробно рассматриваются методы факторизации, а методы DLP и ЭК-порядка кратко описываются с точки зрения их зависимости от факторизации.

Третий параграф главы, озаглавлен **«Актуальные проблемы оценки симметричных и алгоритмов шифрования с открытым ключом»**, в котором анализируются актуальные проблемы оценки симметричных алгоритмов шифрования и алгоритмов шифрования с открытым ключом. В частности, установлено следующее: существующие методы оценки зачастую ограничиваются теоретическими критериями и не в полной мере отражают практическую эффективность; недостаточно изучены возможности построения параметрически оптимизированных моделей алгоритмов шифрования; подходы к оценке на основе машинного обучения и нейронных сетей пока еще не полностью систематизированы. Кроме того, научно обоснована необходимость совершенствования методов анализа нелинейных преобразований для симметричных алгоритмов, а также методы оценки для алгоритмов с открытым ключом, основанных на проблеме факторизации.

Результаты первой главы показали, что существующие подходы к оценке в основном ориентированы на измерение только отдельных характеристик криптосистем и, следовательно, сохраняется высокая потребность в интегрированных, адаптивных и интеллектуальных подходах. Поэтому в последующих главах с целью устранения указанных проблем предложены новые методы оценки, новый метод и алгоритмы анализа нелинейных преобразований, метод и алгоритм классификации ключей шифрования с применением методов машинного обучения, а также алгоритмы определения секретных ключей для алгоритмов шифрования с открытым ключом, построенных на основе проблемы факторизации.

Вторая глава диссертации озаглавлена **«Метод и алгоритм BBKS оценки нелинейных преобразований симметричных алгоритмов шифрования»**, в ней рассмотрены подходы к оценке нелинейных преобразований симметричных алгоритмов шифрования, изучены общие требования к характеристикам нелинейных преобразований, а также предлагается метод под названием **«число совместных появлений битов»**, основанный на статистических характеристиках совместного появления входных и выходных битов в преобразовании; на основе данного метода разработан алгоритм. С использованием разработанного алгоритма выполнена оценка восьми таблиц нелинейных преобразований алгоритма шифрования «Магма».

Первый параграф главы озаглавлен **«Существующие подходы к оценке нелинейных преобразований симметричных алгоритмов шифрования»**, в котором изучаются существующие подходы к оценке симметричных алгоритмов шифрования и критерии анализа характеристик нелинейных преобразований. В симметричных алгоритмах шифрования любое

криптографическое преобразование $X = (x_1, x_2, \dots, x_n)$ в пространстве $GF(2^n)$, можно рассматривать как преобразование $Y = (y_1, y_2, \dots, y_n)$ в другом пространстве $GF(2^m)$, и это преобразование может быть выражено посредством булевых функций следующим образом: $Y = \varphi(X)$: $GF(2^n) \rightarrow GF(2^m), X = (x_1, x_2, \dots, x_n), Y = (y_1, y_2, \dots, y_n)$.

Преобразование представляется в виде векторных булевых функций (компонентов) - $\varphi(X) = \{f_1(X), f_1(X), \dots, f_m(X)\}$. Здесь $f_i, x_i, y_i \in GF(2)$ $(f_i, x_i, y_i = \{0,1\}$. Следовательно, при процессе оценки некоторой криптографической пересатановки в блочно-симметричном алгоритме шифрования достаточно изучить свойства заданной булевой функции, которая является её математической моделью.

Из приведённых понятий ясно, что все вышеуказанные свойства и числовые характеристики преобразований блочно-симметричного алгоритма шифрования оказывают непосредственное влияние на его криптостойкость.

Второй параграф главы озаглавлен **«Метод BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования»**. В данном разделе, помимо ранее существовавших общих характеристик преобразований S-бокса, дополнительно предлагается подход, основанный на изучении вероятности совместного появления входных и выходных битов. С использованием данных подходов определяется степень взаимозависимости между битами внутри S-box.

Сущность метода BBKS можно выразить со следующим определением 1.

Определение 1. Предположим, S - здесь S-box размера n×n, входное значение представляет собой $a \in \{0,1\}^n$, а выходное значение представляет собой $b = S[a] \in \{0,1\}^n$. Тогда число совместных появлений битов определяется следующим образом:

$$c_{p,q}^{i,j}[k,l] = \#\{b_k = p; b_l = q; a_k = i; a_l = j\}$$

Здесь $k = 0, \dots, n-2; l = k+1, \dots, n-1$, $p = 0,1;\ q = 0,1;\ \ i = 0,1; j = 0,1$.

Метод BBKS - этапы оценки нелинейного преобразования S-box

Этап 1. Подготовка входных данных. Выбирается таблица S-box размером $n \times n$. Для каждого входного значения $a \in \{0,1\}^n$ в S-box определяется соответствующее выходное значение $b = S[a] \in \{0,1\}^n$. Все значения представляются в двоичной (binary) форме.

Этап 2. 2-bosqich. Определение пар битов. Для каждой пары битов (a_k, a_l) входного значения рассматриваются все возможные комбинации $(i,j) \in \{0,1\}^2$. Соответственно, для пары битов (b_k, b_l) выходного значения выбираются значения $(p,q) \in \{0,1\}^2$. Этот процесс выполняется для всех пар индексов k, l (т.е. $k = 0, \dots, n-2; l = k+1, \dots, n-1$).

Этап 3. Вычисление числа совместных появлений. Для каждой комбинации пар битов рассчитывается следующая величина:

$$c_{(p,q)]}^{(i,j)}[k,l] = \#\{b_k = p; b_l = q; a_k = i; a_l = j\}$$

Эта величина показывает, насколько часто пары битов $(a_k, a_l) = (i,j)$ во входе соответствуют парам битов $(b_k, b_l) = (p,q)$ на выходе.

Этап 4. Вычисление вероятностей. Для каждого значения определяется вероятность:

$$P_{(p,q)}^{[i,j]}[k,l] = \frac{c_{(p,j)}^{(i,j)}[k,l]}{2^u}$$

Это выражение представляет степень статистической зависимости между входными и выходными битами в виде вероятности.

Этап 5. Анализ результатов. Если все значения $P_{(pq)}^{(i,j)}[k,l]$ близки друг к другу, то биты внутри S-box независимы и равномерно распределены, что указывает на высокую нелинейность и стойкость. Напротив, если для некоторых пар значение $P_{(p,q)}^{(i,j)}[k,l]$ очень велико или мало, это указывает на наличие взаимной зависимости между битами и криптоаналитическую уязвимость S-box.

Результаты используются для совершенствования S-box, разработки новых S-box или оптимизации существующих.

Лемма 2.1 (Свойство равномерного распределения пар битов в методе BBKS). Предположим, $S: \{0,1\}^n \to \{0,1\}^n$ – S-box. Если для каждого входного значения $a \in \{0,1\}^n$ существует выходное значение $b = S[a]$ и все пар битов (a_k, a_l) и комбинации (b_k, b_l) встречаются с одинаковой частотой, то есть:

$$\sum_{a \in \{0,1\}^n} [a_k = i, a_l = j, b_k = p, b_l = q] = \frac{2^{n-2}}{4}$$

таком случае распределение по этим парам битов считается одинаковым.

Теорема 2.1 (Условие независимости битов в методе BBKS). Если выполняется условие леммы 2.1, то есть для каждой комбинации (i, j, p, q, k, l) выполняется:

$$c_{p,q}^{i,j}[k,l] = \frac{2^{n-2}}{4}$$

таком случае если биты -го и l -го порядков в S-box являются взаимно независимыми с статистической стороны.

Это означает, что в 8-м S-box алгоритма шифрования Magma размером 4×4 при условии когда на входном a, бит 1-го порядка равен 0 и 3-го порядка равен 1, количество случаев, когда бит 1-го порядка равен 1 и 3-го порядка равен 1, выходного значения b равно 3. (таблица 1).

Таблица 1.

Число совместных появлений битов (BBKS) в 8-м S-box алгоритма Magma

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	1	0	2	2	1	1	0	0	2	1	1	1	0	2	1
0,2	**3**	1	0	0	0	1	2	1	1	0	2	1	0	2	0	2
0,3	1	1	2	0	0	**3**	0	1	1	0	1	2	2	0	1	1
1,2	1	0	1	2	0	1	1	2	2	0	2	0	1	**3**	0	0
1,3	1	1	2	0	0	0	1	**3**	2	2	0	0	1	1	1	1
2,3	2	2	0	0	1	1	0	2	1	0	2	1	0	1	2	1

Метод BBKS предлагает новый подход для анализа свойств нелинейных преобразований S-box на уровне битов. В то время как традиционные методы алгебраического, дифференциального или линейного анализа больше ориентированы на общую структуру S-box, подход BBKS определяет степень внутренней зависимости через оценку вероятности совместного появления входных и выходных битов. Это даёт более глубокую информацию о статистической независимости и распределении S-box. Если взаимная зависимость между битами минимальна, такой S-box демонстрирует относительно высокую стойкость.

Третий параграф главы озаглавлен **«1-алгоритм, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования»,** в котором описан алгоритм 1, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования.

1-алгоритм. *алгоритм 1, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования.*

Шаг 1. Для случайных входных значений выполняется несолько процессов шифрования. Процесс продолжается до тех пор, пока не будет сформирован массив, в котором все возможные варианты битов, соответствующих S-box, для L_n, R_n встречаются ровно один раз, то есть значения не повторяются. Такие массивы формируются при выполнении процесса шифрования на одинаковом значении L_{n-1}.

Шаг 2. Полученный массив R_n объявляется в качестве S-box, после чего вычисляется число совместных появлений битов внутри этого S-box.

Шаг 3. Значение L_{n-1} определяется путём сложения по операция XOR соответствующих значений BBKS из таблицы, отражающие число совместных появлений битов в S-box, использованного в процессе шифрования, и значений BBKS, вычисленных для массива R_n.

Шаг 4. Используя имеющиеся значения L_{n-1}, L_n, R_n значение K_n определяется выражением $L_{n-1} \oplus S(L_n \oplus K_n) = R_n$.

Шаг 5. Полученное значение K_n объявляется в качестве предполагаемого ключа -го раунда.

Таблица 2.

Число совместных появлений битов в таблице S-box, сформированной из значений массива R_n.

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	2	1	1	0	1	1	1	1	1	0	2	1	0	2	1	1
0,2	2	0	1	1	1	2	0	1	1	2	1	0	0	0	1	**3**
0,3	1	1	2	0	1	2	1	0	0	1	0	**3**	2	0	1	1
1,2	**3**	1	0	0	0	2	0	2	1	1	1	1	0	1	2	1
1,3	1	1	1	1	2	2	0	0	1	0	0	**3**	1	1	2	0
2,3	1	1	1	1	2	1	1	0	0	2	1	1	0	0	2	2

В результате вычислений, выполненных в соответствии с условиями Шага 1, были получены массивы L_n=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15] и R_n

=[8, 1, 6, 3, 12, 0, 5, 14, 9, 2, 15, 10, 7, 4, 13, 11]. На основании Шага 2 массив R_n объявляется S-box, после чего вычисляется число совместных появлений битов в этом S-box.

Таблица 4.

Определение значения L_{n-1} с использованием соответствующих значений из таблиц числа совместных появлений битов.

Позиции битов	**Значения в S-box**	**Соответствующие значения массива R_n**	**Результат XOR соответствующих значений**	**0-бит**	**1-бит**	**2-бит**	**3-бит**
0,2	0,0	1,1	1,1	1	-	1	-
0,3	0,1	1,1	1,0	1	-	-	0
1,2	0,1	0,0	0,1	-	0	1	-
1,3	1,1	1,1	0,0	-	0	-	0
0,2	0,1	1,0	1,1	1	-	1	-
0,3	1,1	0,1	1,0	1	-	-	0
1,2	0,0	0,1	0,1	-	0	1	-
1,3	1,0	0,0	1,0	-	1	-	0
Полученное значение L_{n-1}:				**1**	**0**	**1**	**0**

На основе шага 3 значение L_{n-1} определяется с использованием значений из таблицы 2, соответствующих выходным битам {0,2},{0,3},{1,2},{1,3}, представляющии число совместных появлений битов в таблице S-box, использованной в процессе шифрования (Таблицу 3).

Согласно Шагу 4, после определения значения L_{n-1} значение K_n вычисляется по следующему выражению:

$$L_{n-1} \oplus S(L_n \oplus K_n) = R_n \qquad (1)$$

Это выражение является уместным для любых значений массива L_n и соответствующих им значений массива R_n.

Если $L_n = 0_{10} = 0000_2$ то соответствующее значение массива R_n равно $R_n = 8_{10} = 1000_2$. Подставив эти значения в выражение (1) и определённое значение $L_{n-1} = 10_{10} = 1010_2$, можно получить выражение $1010 \oplus S(0000 \oplus K_n) = 1000$. Из этого можно определить, что $S(0000 \oplus K_n) = 0010$ и значение ключа $K_n = 1111$ с помощью Таблицы 1.

Четвёртый параграф главы озаглавлен **«Алгоритм 2, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования»**, в котором в котором описан алгоритм 2, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования.

2-алгоритм. *алгоритм 2, разработанный на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования.*

Шаг 1. Процесс шифрования выполняется до тех пор, пока не будут получены все возможные значения L_n, при условии, что все значения массива R_n принимают одинаковое значение (например, все значения равны 0 или 1).

Шаг 2. Полученный массив L_n объявляется в качестве S-box, после чего вычисляется число совместных появлений битов внутри этого S-box.

Шаг 3. Формируется таблица числа совместных появлений битов для S-box_inv, которая является обратной таблице S-box, используемой в процессе шифрования.

Шаг 4. Значение K определяется путём сопоставления таблиц BBKS для сформированного S-box_inv и массива L_n то есть путём сложения соответствующих битов по операция XOR.

Шаг 5. Полученное значение K_n объявляется в качестве предполагаемого ключа -го раунда.

Ключ в процессе шифрования (Таблица 7) определяется путем сопоставления числа совместных появлений битов массива L_n (Таблица 6) с числом совместных появлений битов таблицы S-box_inv (Таблица 5).

Таблица 5.

Числа совместных появлений битов в S-box_inv для обратной таблице 8-го S-box

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	2	0	1	1	1	2	0	0	1	1	2	2	0	1	1
0,2	**3**	0	1	0	1	1	0	2	0	2	2	0	0	1	1	2
0,3	1	0	1	2	1	**3**	0	0	2	0	1	1	0	1	2	1
1,2	1	0	2	1	0	1	0	**3**	1	1	2	0	2	2	0	0
1,3	1	0	2	1	1	0	2	1	2	1	1	0	0	**3**	0	1
2,3	2	1	1	0	2	1	0	1	0	0	2	2	0	2	1	1

Таблица 6.

Число совместных появлений битов массива L_n

	0,0				**0,1**				**1,0**				**1,1**			
	0,0	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**	**0,0**	**0,1**	**1,0**	**1,1**
0,1	1	0	2	1	0	2	1	1	2	1	1	0	1	1	1	1
0,2	0	1	0	**3**	2	0	1	1	0	2	2	0	2	1	0	1
0,3	2	1	0	1	0	0	**3**	1	1	1	0	2	1	2	1	0
1,2	1	2	0	1	**3**	0	1	0	0	2	1	1	0	1	1	2
1,3	1	2	0	1	1	2	0	1	1	1	1	1	1	0	**3**	1
2,3	0	1	1	2	1	0	1	2	2	1	0	1	1	1	2	0

Таблица 7.

Определение значения K_n с использованием соответствующих значений из таблиц числа совместных появлений битов

Позиции битов	**Значения в S-box_inv**	**Соответствующие значения массива L_n**	**Результат XOR соответствующих значений**	**0-бит**	**1-бит**	**2-бит**	**3-бит**
0,2	0,0	1,1	1,1	1	-	1	-
0,3	0,1	1,0	1,1	1	-	-	1
1,2	1,1	0,0	1,1	-	1	1	-
1,3	0,1	1,0	1,1	-	1	-	1
0,2	1,0	0,1	1,1	1	-	1	-
0,3	0,0	1,1	1,1	1	-	-	1
1,2	0,1	1,0	1,1	-	1	1	-
1,3	1,1	1,1	0,0	-	0	-	0
Полученное значение K_n:				**1**	**1**	**1**	**1**

Процесс определения того, что $K_n=1111_2$ является ключевыми битами, использованными в процессе шифрования, является достаточно простым.

Третья глава диссертации озаглавлена **«Метод и алгоритм факторизации на основе правила умножения чисел для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации».** В этой главе изучены ускоренные методы умножения чисел, а для алгоритмов открытого ключа, основанных на проблеме факторизации, разработан новый метод факторизации KATAOF, основанного на методе умножения чисел Тоома-Кука. Были разработаны два алгоритма факторизации: KATAOF-1 и KATAOF-2, на основе нового метода KATAOF основанного на методе умножения чисел Тоома-Кука для алгоритмов открытого ключа, основанных на проблеме факторизации.

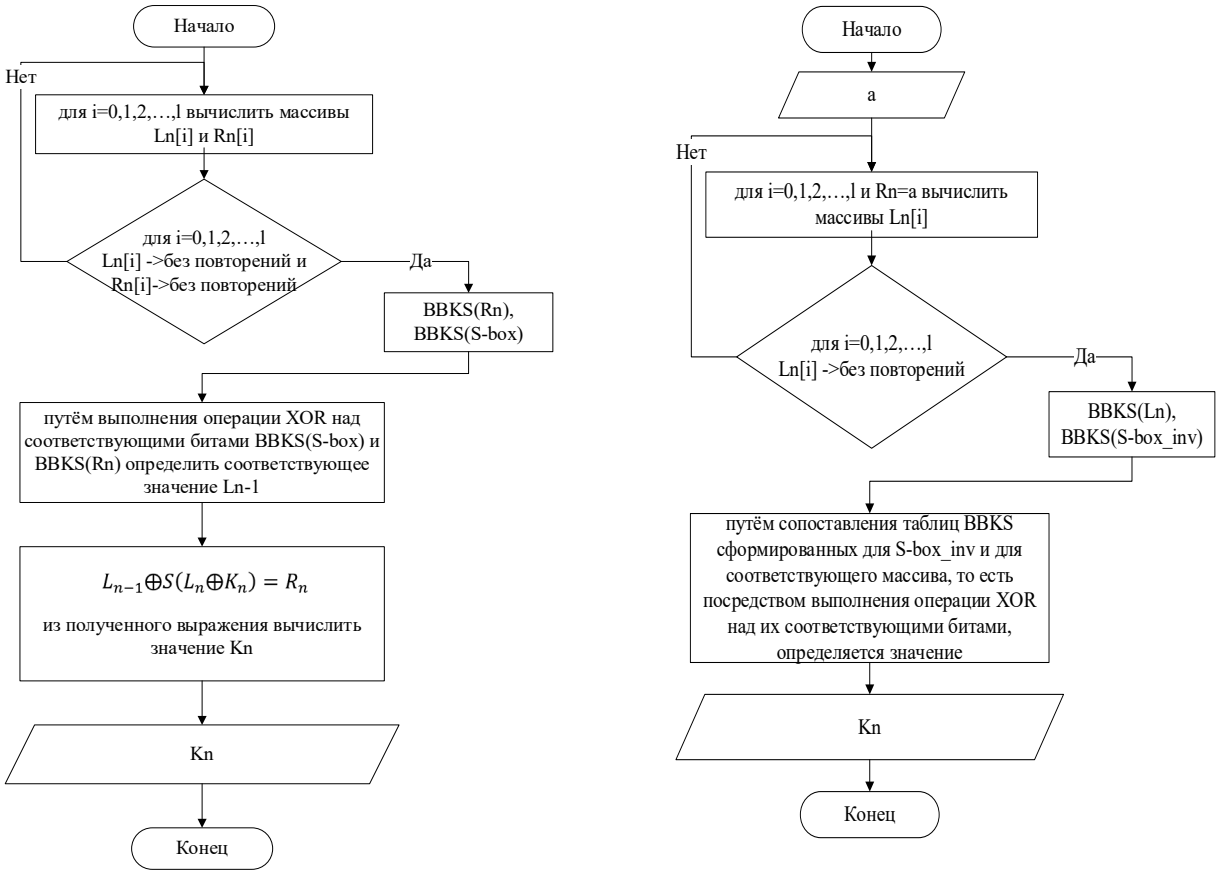


Рисунок 1. Блок-схема Алгоритмов 1 и 2, разработанных на основе метода BBKS для оценки нелинейного преобразования симметричных алгоритмов шифрования.

Первый параграф главы озаглавлен **«Быстрые методы умножения чисел и их применение»**. Умножение чисел является одной из ключевых операций арифметики. При работе с большими числами, особенно в криптографии, цифровой обработке сигналов, компьютерной графике и алгоритмических вычислениях, скорость умножения напрямую влияет на эффективность вычислений. По этой причине на протяжении истории математики было разработано множество методов для ускорения умножения. В данном параграфе рассмотрены математические методы, такие как алгоритмы Карацубы, Karatsuba, Toom-Cook, Schonhage-Strassen, Harvey & van

der Hoeven, Booth кодирование, Wallace и деревья Dadda, библиотеки GMP/MPIR.

Различные быстрые алгоритмы умножения чисел - методы Karatsuba, Toom-Cook, Schonhage-Strassen и Furye - с математической точки зрения они важны не только для ускорения арифметических операций, но и имеют теоретическое значение в криптоаналитических процессах, особенно при решении проблем факторизации. Потому что в основе факторизации лежит произведение вида N=p×q, то есть при обратной операции - разложении произведения на множители - требуется глубокое изучение структуры и свойств умножения.

В результате быстрые методы умножения рассматриваются не только как математический инструмент для оптимизации вычислений, но и как направление, открывающее новые теоретические основы для решения сложных задач, таких как факторизация и криптоанализ. По этой причине глубокое изучение механизмов умножения чисел является важным научным направлением для оценки надёжности современных криптосистем и разработки новых быстрых моделей факторизации.

Второй параграф главы озаглавлен **«Метод факторизации KATAOF, основанный на методе умножения чисел Тоома-Кука».** В этом параграфе диссертации изучена возможность решения задачи факторизации с использованием шагов алгоритма Тоома-Кука, основанного на умножении чисел и многочленов. На основе результатов исследования освещены методы, направленные на эффективное выполнение процесса факторизации, а также применение алгоритмов, разработанных на основе этих методов.

Метод факторизации KATAOF, основанный на методе Тоом-Кука умножения чисел

Входные данные:

N – число, подлежащее факторизации;

k - длина числа в битах;

l - длина каждого фрагмента в битах;

$m = n/l$ - количество формируемых фрагментов.

Шаг 1. Разделение числа на фрагменты. Число N делится на $m = n/l$ фрагментов по l бит:

$$N = [n_{m-1}, n_{m-2}, \dots, n_1, n_0]$$

здесь, каждый $n_i - l$- битовый фрагмент числа N.

Шаг 1. Определение начальных кандидатных пар

Для рассматриваемых простых чисел p и q:

$$p = \left[p_{k/l-1}, \dots, p_1, p_0\right], q = \left[q_{k/l-1}, \dots, q_1, q_0\right]$$

Шаг 2. Для каждого значения n_i с помощью операций обратных правилу умножения определяются соответствующие кандидатные пары (p_i, q_i).

Шаг 3. Расширение кандидатных пар. Начиная с определённых начальных пар p_0, q_0, рекурсивно формируются следующие пары:

$$\left(p^i, q^i\right), i = 0,1,2, \dots, 2^{k-2} - 1.$$

В результате формируется множество потенциальных пар 2^{k-2}.

Шаг 4. Проверка равенства. Для каждой кандидатной пары проверяется следующее условие:

$$p^i \times q^i = N.$$

Если равенство не выполняется, проверка продолжается для следующей пары.

Шаг 5. Завершение. Если для некоторого i выполняется равенство $p^i \times q^i = N$, то присваивается $p = p^i, q = q^i$ и они объявляются искомыми простыми числами. Алгоритм завершает свою работу.

Выходные значения: $(p, q) - N$ объявляются простыми делителями числа.

Третий параграф главы озаглавлен **«Алгоритмы факторизации KATAOF, основанные на методе умножения чисел Тоома-Кука»**. На основе метода факторизации, основанного на методе умножения чисел Тоома-Кука, предложенном в параграфе 3.2 алгоритм разложения числа N, являющегося произведением двух -битных простых чисел p и q, может быть описан следующим образом.

Блок-схема алгоритма KATAOF-1, разработанного на основе метода факторизации, построенного на методе умножения чисел Тоома-Кука, приведена на рисунке 2.

Блок-схема алгоритма KATAOF-2, разработанного на основе метода факторизации, построенного на методе умножения чисел Тоома-Кука, приведена на рисунке 3.

Данный метод факторизации, основанный на методе умножения Тоома-Кука, открывает новые возможности при анализе больших чисел. Этот подход является одним из перспективных методов, пригодных для практического применения в задачах факторизации криптографических модулей большой разрядности, оценки безопасности RSA и в области математического криптоанализа.

В данной главе предложен эффективный метод MOKM для модулей RSA малой разрядности, основанный на соотношении между открытым и секретным ключами, для определения секретного ключа алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации. Кроме того, для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, разработан метод определения секретных ключей, названный «методом сближения квадратов целых квадратных корней» (BKIKYU) и разработан алгоритм на основе метода BKIKYU определения секретных ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации.

Четвёртая глава диссертации озаглавлена «Методы и алгоритм на основе соотношения ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации».

Первый параграф главы озаглавлен «Метод MOKM, основанный на соотношении открытого и секретного ключей, для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации». Ниже приведено общее описание метода MOKM

определения секретного ключа $p, q \in (a, b)$ $\varphi(N) = (p-1) * (q-1)$ $(p, q \in (a, b))$ с использованием заданного открытого ключа e и чисел $N = p * q$ в алгоритме шифрования RSA.

Метод 4.1. Метод МОКМ определения секретного ключа алгоритма шифрования RSA.

1. Интервал (a, b) разбивается на малые части;

2. Определяется, к каким из выделенных частям могут принадлежать числа p, q;

3. Для частей, определённых на шаге 2, вычисляется диапазон значений $r \in [\frac{2\cdot(\left[\frac{N''}{2}\right]-[\sqrt{N''}])-\varphi''(N'')}{2}, \frac{2\cdot(\left[\frac{N'}{2}\right]-[\sqrt{N'}])-\varphi'(N')}{2}]$, $N' = p_{min} \cdot q_{max}$, $\varphi'(N') = (p_{min}-1)\cdot(q_{max}-1), N'' = p_{min} \cdot q_{min}$, $\varphi''(N'') = (p_{min}-1)\cdot(q_{min}-1)$ p_{min}, q_{max};

4. Для $\varphi(N) = 2 \cdot (\left[\frac{N}{2}\right] - \left[\sqrt{N}\right] - r)$ вычисленного с использованием значений r из диапазона, определенном на шаге 3, вычисления прекращаются, если выполняется равенство $m^e \ mod \ n = m^{e+\varphi(N)} \ mod \ N$.

5. Значение $\varphi(N)$, удовлетворяющее равенству на шаге 4, объявляется искомым секретным ключом.

Приведённый метод подтверждает свою эффективность для простых чисел p и q малой разрядности на основе экспериментальных результатов. При этом суть алгоритма заключается в том, что, опираясь на модуль $N = p \times q$, осуществляется косвенное определение значения функции $\varphi(N)$ и, соответственно, проверка соотношений шифрования-дешифрования.

Эффективность представленного метода зависит от разбиения интервала (a, b) на как можно меньшие интервалы и от точности определения того, в каком интервале находятся искомые простые числа p и q. Эффективность этого метода значительно повысится, если будет найден оптимальный способ разбиения интервала (a, b) на более мелкие интервалы и определения того, в каком интервале находятся искомые числа p и q, или если будет определена взаимосвязь между числом r и числом N.

Второй параграф главы озаглавлен **«Метод BKIKYU определения секретных ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации».** В этом параграфе изучается сложность факторизации модуля, составляющего основу безопасности алгоритма RSA. Показано, что когда модуль $N = p * q$ имеет длину l бит, если разница простых множителей удовлетворяет условию $|p - q| \leq 2^{l/4}$, то факторизация модуля может быть выполнена существенно быстрее по сравнению с традиционными методами. В предложенном методе BKIKYU процесс поиска ограничивается порядком $l/2$ шагов, что обеспечивает возможность факторизации модуля за сравнительно короткое время.

Теорема 4.2 (Близость квадратных корней $\varphi(N)$ и N для RSA-модуля). Пусть задан RSA-модуль $N = p \cdot q$, где p и q — различные простые числа, при $p > q$, $\sqrt{N} - 2 < \sqrt{\varphi(N)} < \sqrt{N} - 1$, с точки зрения всей части будут уместными соотношение близости: $\left|\sqrt{\varphi(N)}\right| = \left|\sqrt{N}\right| - 1$ или $\left|\sqrt{\varphi(N)}\right| =$

$\left|\sqrt{N}\right| - 2$

На основе данного математического обоснования был предложен метод сближения квадратов целых квадратных корней (BKIKYU). Этапы поиска секретного ключа по методу БКИКЮ приведены ниже.

Этап 1. Подготовка исходных значений. Для заданного числа N вычисляются следующие:

$$r = \lfloor\sqrt{N}\rfloor^2, r_p = \lfloor\sqrt{N} - 1\rfloor^2$$

Эти значения выбираются как два квадратных числа, близких к N.

Этап 2. Определение приближённого значения $\varphi(N)$. На каждой итерации вычисляется среднее значение:

$$t = \sqrt{r \cdot r_p}$$

Полученное значение t принимается в качестве приближённой оценки $\varphi(N)$.

Этап 3. Вычисление дискриминанта. На основе приближённого значения $\varphi(\mathrm{N})$ определяются соответствующие величины.

$$s = N - \varphi(N) + 1, D = s^2 - 4N$$

Этап 4. Анализ дискриминанта. Если $\mathrm{D} < 0$ дискриминант отрицателен, то действительных корней не существует; в этом случае верхняя граница заменяется значением t и если условие $\left|\mathrm{r} - \mathrm{r_p}\right| \leq 2$ не выполняется, выполняется возврат к этапу 2, в противном случае переходят к этапу 5. Если $D \geq 0$, извлекается квадратный корень дискриминанта $\sqrt{D}$, и после определяются значения p и q следующим образом:

$$p = \frac{s + \left|\sqrt{D}\right|}{2}, q = s - p$$

Если выполняется условие $p \cdot q = N$, процесс завершается. В противном случае значение нижней границы заменяется на t, и если условие $\left|r - r_p\right| \leq 2$ не выполняется, выполняется возврат к этапу 2.

Этап 5. По завершении процедуры возвращается последнее вычисленное значение t. Итоговое значение $\varphi(N)$ ищется в следующем интервале:

$$\varphi(N) \in \{t - 1, t, t + 1\}$$

С использованием данного метода::

находится приближённое значение $\varphi(\mathrm{N})$;

затем определяются p и q;

в результате становится возможным вычислить секретный ключ $d = e^{-1}\mathrm{mod}\varphi(N)$алгоритма RSA.

Эффективность метода наиболее высока в случаях, когда значения p и q взаимно близки. Если при $p \approx q$ значение $\varphi(N)$ может быть быстро определено по отношению к N за счёт сближения квадратных корней.

Третий параграф главы озаглавлен «Алгоритм BKIKYU определения секретных ключей для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации». На основе метода BKIKYU, приведённого в разделе 4.1, также разработан алгоритм «метода сближения целых квадратных корней» (BKIKYU). Основная цель

разработанного алгоритма БКИКЮ - разложение RSA-модуля $N = p \cdot q$ на его простые множители p и q. Алгоритм разделён на две подалгоритмические части. Сначала алгоритм *BKIKYU(N)* предназначен для нахождения приблизительного значения $\varphi(N)$ (функции Эйлера), а последующий алгоритм *find_pq_from_phi_candidates(N, t)* на основе этого значения выполняет определение p и q (рис. 2).

При разработке метода и алгоритма сближения квадратов целых квадратных корней была установлена и доказана следующая теорема.

Теорема 4.3. Предположим, что $N = pq$ произведение двух нечётных простых чисел, а $l-$битовая длина числа N, (то есть $2^{l-1} \le N < 2^l$). Если $|p - q| \le 2^{[I/4]}$ то $\varphi(N) = N - 1 - 2 * \lfloor\sqrt{N}\rfloor$ т. е. если $m = \lfloor\sqrt{N}\rfloor$ то справедливо $\varphi(N) = N - 1 - 2m$.

Хотя методы Ферма, Полларда и Шэнкса эффективны для чисел малой и средней битовой длины, с увеличением разрядности вычислительная сложность резко возрастает. Алгоритм решета числового поля (NFS) в настоящее время признан наиболее мощным универсальным методом и применяется для факторизации крупных RSA-чисел. Предложенный алгоритм, основанный на разбиении на интервалы, при выполнении условия $|p - q| \le 2^{l/4}$ обеспечивает быстрый результат независимо от битовой длины и позволяет за короткое время определить значения $\varphi(N), p, q$. Данное свойство делает его более предпочтительным по сравнению с другими алгоритмами.

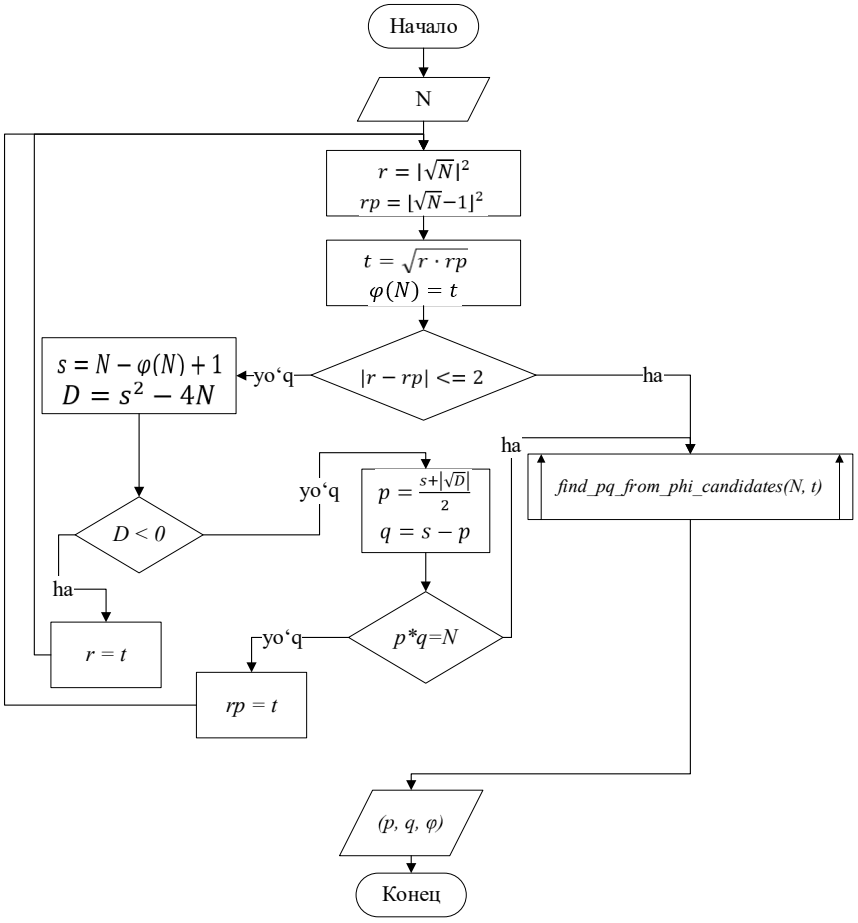


Рисунок 2. Блок-схема алгоритма BKIKYU

Эксперименты, проведённые на модулях длиной 4095 и 4096 бит, наглядно продемонстрировали эффективность предложенного алгоритма. В частности, для N длиной 4095 бит алгоритм завершил вычисление $\varphi(N)$, за 0,000248 с, а для N длиной 4096 бит - за 0,000255 с. Полученные результаты свидетельствуют о принципиально высокой вычислительной скорости предложенного подхода: поскольку процесс факторизации сводится к нескольким простым арифметическим операциям, таким как вычисление целочисленного квадратного корня и проверка дискриминанта, он завершается за крайне короткий промежуток времени.

Пятая глава диссертации озаглавлена **«Результаты оценки эффективности разработанных методов и алгоритмов»**. В данной главе выполнена оценка эффективности методов и алгоритмов, предложенных в ходе исследования. В частности, проанализировано взаимодействие метода BBKS с существующими общими криптографическими требованиями, а также его влияние на устойчивость нелинейных преобразований к криптоаналитическим атакам. Кроме того, проведено сравнительное сопоставление с точки зрения вычислительной сложности методов KATAOF, MOKM и BKIKYU разработанных для оценки алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, и соответствующих алгоритмов, созданных на их основе, с другими алгоритмами данного типа.

Первый параграф главы озаглавлен **«Влияние метода BBKS на устойчивость нелинейных преобразований»**. Согласно BBKS анализу, для S-box размерности 4×4 характеристика BBKS в первую очередь в заметной степени зависит от структурных свойств, в частности от наличия фиксированных точек (FP) и противоположных фиксированных точек (OFP).

В S-box алгоритма «Magma» при наличии значений FP и OFP число отклонений по BBKS находится в диапазоне 1–5, что свидетельствует о нарушении баланса распределения. Напротив, для групп S-Box1–S-Box5 и S-Box9–S-Box20, где FP=0 и OFP=0, отклонения по BBKS равны 0, то есть 2-битные пары вход-выход распределены равномерно.

Также установлено, что показатель BBKS имеет умеренную корреляцию со свойством строгого лавинного эффекта (SAC). При этом по мере приближения значения SAC к 0,5 наблюдается увеличение числа отклонений по BBKS, тогда как для S-box со значениями SAC ≈ 0.625–0.656 показатель BBKS приближается к оптимальному. Однако, поскольку для всех рассмотренных S-box значения нелинейности (NL=4), корреляционной иммунности (CI=0) и алгебраической степени (AI=2) совпадают, можно сделать вывод, что показатель BBKS не находится в прямой зависимости от этих параметров. Следовательно, показатель BBKS в основном определяется локальной структурной симметрией и дифференциальной сбалансированностью, тогда как с общими показателями нелинейности он напрямую не связан. Результаты анализа приведены в таблице 8.

Таблица 8.

Результаты оценки S-box- размерности 4×4 по общим криптографическим требованиям и характеристика BBKS

S-box	B	SAC (=0.5)	FP	OFP	Big_SAC (=0.5)	NL	CI	AI	BBKS (число отклонений)
Magma_1	+	0.5156	1	0	0.520	4	0	2	1/3 (5)
Magma_2	+	0.5469	4	1	0.510	4	0	2	1/3 (2)
Magma_3	+	0.5156	1	0	0.541	4	0	2	1/3 (1)
Magma_4	+	0.5312	2	2	0.541	4	0	2	1/3 (3)
Magma_5	+	0.5625	2	0	0.510	4	0	2	1/3 (0)
Magma_6	+	0.5459	1	1	0.552	4	0	2	1/3 (3)
Magma_7	+	0.5938	1	1	0.531	4	0	2	1/3 (1)
Magma_8	+	0.5	2	0	0.562	4	0	2	1/3 (4)
Present	+	0.625	0	1	0.562	4	0	2	1/3 (0)
S-Box1	+	0.500	0	0	0.500	4	0	2	1/3 (2)
S-Box2	+	0.500	0	0	0.500	4	0	2	1/3 (4)
S-Box3	+	0.500	0	0	0.500	4	0	2	1/3 (3)
S-Box4	+	0.500	0	0	0.500	4	0	2	1/3 (4)
S-Box5	+	0.640	0	0	0.541	4	0	2	1/3 (0)
S-Box6	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box7	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box8	+	0.640	0	1	0.541	4	0	2	1/3 (0)
S-Box9	+	0.640	0	0	0.552	4	0	2	1/3 (0)
S-Box10	+	0.656	0	0	0.520	4	0	2	1/3 (0)
S-Box11	+	0.640	0	0	0.541	4	0	2	1/3 (0)
S-Box12	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box13	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box14	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box15	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box16	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box17	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box18	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box19	+	0.625	0	0	0.562	4	0	2	1/3 (0)
S-Box20	+	0.625	0	0	0.562	4	0	2	1/3 (0)

Второй параграф главы озаглавлен **«Вычислительная сложность метода KATAOF».** В данном параграфе показано, что вычислительная сложность метода KATAOF равна $O\left(2^{\frac{k}{2}-2}\right)$.

Третий параграф главы озаглавлен **«Вычислительная сложность метода MOKM».** В данном параграфе показано, показано, что вычислительная сложность метода MOKM равна равна $O\left(2^{k/(2^t)}\right)$.

Четвёртый параграф главы озаглавлен **«Вычислительная сложность метода BKIKYU»**. В данном параграфе установлено, что вычислительная

сложность метода BKIKYU равна $|p-q| \le 2^{\frac{l}{4}}$ da $O(l/2)$ va $|p-q| > 2^{\frac{l}{4}}$ da $O\left(2^{l/2} \cdot l\right)$.

Сравнительный анализ алгоритмов факторизации по вычислительной сложности приведён в таблице 9.

Таблица 9.

Сравнительный анализ алгоритмов факторизации

Метод/ алгоритм	**Основа**	**Предел эффективности**	**Вычислительная сложность**	**Примечание**
Метод факторизации Ферма	Представление в виде $N = x^2 - y^2$	Очень эффективен при p ≈ q, общем случае ~130–150 bit t	$O\left(N^{1/2}\right)$ в лучшем случае $O\left(N^{1/4}\right)$	Применим в основном для близких факторов
Алгоритм Полларда ρ	Итерационная функция, обнаружение цикла и парадокс «дня рождения»	эффективен для чисел порядка ~40–60 десятичных знаков (примерно 130–200 бит)	$O(N^{1/4})$	Наиболее эффективен как вероятностный метод для поиска малых простых делителей
Алгоритм Полларда–Штрассена	комбинация ρ + FFT (Strassen)	~150–200 бит	$O(N^{\frac{1}{4}} * log_4 N)$	На практике может работать быстрее, чем алгоритм Полларда ρ\rhoρ, однако его эффективность на больших числах ограничена
Метод Шэнкса: SQUFOF	Поиск близких корней с использованием квадратичных форм	хорошо работает до чисел порядка ~100 десятичных знаков (≈ 330 бит)	$O(N^{\frac{1}{4}+\varepsilon})$	Благодаря относительно низкой сложности эффективен для чисел средней разрядности, однако по мере увеличения битовой длины его скорость резко снижается.
Алгоритм Полларда p−1	если p−1 разлагается на малые факторы	p если p−1 разлагается на малые факторы	$O(N^{\frac{1}{4}} * log^c N)$	Быстро работает для специальных простых делителей
Алгоритм Лемана	детерминированный поиск по квадратному корню	до чисел порядка ~20–25 десятичных знаков (примерно 70–85 бит)	$O(N^{1/3})$	Интересно в теории, на практике заменено на QS.
Алгоритм Диксона	Накопление квадратичных конгруэнций	до чисел порядка ~100 десятичных знаков (≈ 330 бит)	$L_N(\frac{1}{2}, 2\sqrt{2})$	Предыдущий этап QS
Метод непрерывных дробей (CFRAC)	Использование дробных приближений	до чисел порядка ~110–120 десятичных знаков (≈ 360–400 бит)	$L_N(\frac{1}{2}, 2\sqrt{2})$	Уступил место для QS
Квадратичное решето (QS/MPQS)	Обобщённая форма метода Ферма	эффективен до чисел порядка ~120–130	$L_N(\frac{1}{2}, 1)$	до появления GNFS считался самым быстрым

Метод/ алгоритм	Основа	Предел эффективности	Вычислительная сложность	Примечание
		десятичных знаков (≈ 400–430 бит)		универсальным методом
Lenstra ECM (Elliptic Curve Method)	Специализированная факторизация на основе эллиптических кривых	эффективно выделяет простые множители разрядностью 200–400 бит	$L_p(\frac{1}{2}, 2\sqrt{2})$, p – наименьший простой делитель	Наиболее эффективен для малых и средних простых делителей
Метод NFS	просеивание в алгебраических/числовых полях; в настоящее время - наиболее мощный универсальный алгоритм	наилучший выбор для чисел порядка 200 десятичных знаков (≈ 660 бит) и более	$L_N(\frac{1}{3}, \sqrt[3]{\frac{64}{9}})$	В настоящее время - самый быстрый универсальный алгоритм факторизации; все крупнейшие факторизации RSA-рекордных чисел выполнены с использованием данного метода
Метод и алгоритм BKIKYU, предложенные в данной работе	$[\sqrt{N} - 1^2, \sqrt{N}]$ основанный на равномерном делении интервала, основанный на условии $\lvert p - q \rvert \leq 2^{l/4}$	при выполнении условия $\lvert p - q \rvert \leq 2^{l/4}$ ограничение по битовой длине отсутствуе l - *длина числа* N	возможность быстрой факторизации за $O(\frac{l}{2})$, $l/2$ шагов	если условие не выполняется, погрешность алгоритма $\lvert p - q \rvert \leq 2^{\ell/4}$ равно $p + q - 2 * \sqrt{N} \pm 2$ ga teng bo‘ladi.

ОБЩИЕ ВЫВОДЫ

Исходя из поставленной в диссертационной работе цели и задач, получены следующие результаты:

1. Разработан новый метод оценки нелинейных преобразований симметричных алгоритмов шифрования, называемый «число совместных появлений битов». Данный метод служит дополнительным требованием к существующим общим криптографическим критериям при оценке S-box-преобразований и нелинейные преобразования позволяет определять ключи шифрования на основе порядка повторений совместных появлений входных битов на выходе.

2. На основе нового метода оценки нелинейных преобразований симметрических алгоритмов шифрования, называемого «число совместных появлений битов», разработаны два алгоритма определения ключа шифрования, данные алгоритмы позволили оценить секретный ключ с точностью до 75%, соответствующего S-box-преобразованиям размерности 4×4 и со 100% точностью для некоторых S-box.

3. Разработан новый метод факторизация KATAOF посредством обратных операций к умножению, основанный на методе умножения Тоома-Кука, для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, данный метод позволяет факторизацию на основе соотношений, возникающих при умножении чисел.

4. На основе метода KATAOF, построенного на методе умножения Тоома-Кука, для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, были разработаны два алгоритма факторизации - KATAOF-1 и KATAOF-2, данные алгоритмы позволяют факторизовать модуль -битного алгоритма шифрования с открытым ключом RSA при наличии доступного объёма памяти порядка $2^{\frac{l}{2}-2}$;

5. Разработан метод MOKM определения секретного ключа алгоритмов шифрования с открытым ключом основанный на проблемы факторизации и учитывающий соотношения секретного и открытого ключей, эффективный в малобитных модулях RSA, данный метод позволяет определить секретный ключ при успешном прогнозировании того, к каким интервалам могут принадлежать простые числа p и q;

6. Разработан метод определения секретных ключей, названный метод сближения квадратов целых квадратных корней (BKIKYU) для алгоритмов шифрования с открытым ключом, основанных на проблеме факторизации, на основе данного метода разработан алгоритм, данный алгоритм позволяет обнаруживать секретные ключи при l -битном модуле алгоритма шифрования с открытым ключом *RSA* и при выполнении условия $|p - q| \leq 2^{\frac{l}{4}}$, затрачивая порядка $\frac{l}{2}$.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.03/2025.27.12.FM.01.03 NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN

BOYKUZIEV ILKHOM MARDANOKULOVICH

EVALUATION METHODS AND ALGORITHMS FOR SYMMETRIC AND PUBLIC-KEY ENCRYPTION ALGORITHMS

05.01.05 – Methods and systems of information protection. Information and cybersecurity

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

Tashkent-2026

The theme of dissertation of doctor of physical and mathematical sciences (DSc) was registered at the Supreme attestation comission at the Ministry of higer education, science and innovation of the Republic of Uzbekistan under number B2026.DSc/FM316.

Dissertation has been prepared at National University of Uzbekistan.

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

Scientific adviser:	**Abdurakhimov Bakhtiyor Fayzievich** Doctor of physical and matematical sciences, professor
Official opponents:	**Kuryazov Davlatyor Matyakubovich** Doctor of physical and matematical sciences
	Tuychiev Gulom Numonovich Doctor of physical and matematical sciences
	Botirov Fayzullajon Bakhtiyorovich Doctor of technical sciences, docent
Leading organization:	**The Military Institute of Information and Communication Technologies and Communications of the Ministry of Defense of the Republic of Uzbekistan**

Defense will takr place "____" _____ 2026 at ____ ft the meeting of Scientific Council number DSc.03/2025.27.12.FM.01.03 at National University of Uzbekistan. (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 227-12-24, fax: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

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

Abstract of dissertation sent out on "____" _____ 2026 year
(Mailing report №_____ on "____"_____2026 year)

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

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

A.V. Kabulov
Chairman of Scientific seminar under scientific council on award of scientific degress, D.T.S., professor

INTRODUCTION (abstract of DSc dissertation)

The aim of the research is to develop solutions based on new approaches for evaluating the security of symmetric and public-key encryption algorithms.

The object of the research is symmetric and public-key encryption algorithms.

The scientific novelty of the research is as follows:

a method for evaluating nonlinear transformations in symmetric encryption algorithms has been developed, enabling the determination of encryption keys based on the order of repetition of joint occurrences of input bits at the output of nonlinear transformations and serving as an additional requirement to existing general cryptographic criteria in the evaluation of S-box transformations;

algorithms for determining encryption keys based on the method for evaluating nonlinear transformations in symmetric encryption algorithms have been developed, which allow estimation of the secret key with an accuracy of up to 75% for 4×4 S-box transformations and with 100% accuracy for certain S-boxes;

a factorization method based on inverse operations to multiplication has been developed, relying on the Toom–Cook multiplication method and enabling factorization based on relationships arising during the multiplication of numbers;

new factorization algorithms based on the method developed from the Toom–Cook multiplication approach have been proposed, enabling the factorization of an l-bit modulus of the RSA cryptosystem under the condition of sufficient memory of order $2\hat{}(\mathrm{l}/2-2)$;

an efficient method for determining the secret key in small-bit RSA moduli has been developed, taking into account the relationships between the secret and public keys in public-key encryption algorithms based on the factorization problem, allowing the determination of the secret key when it is possible to predict the intervals to which the prime numbers p and q may belong;

a method for determining secret keys for public-key encryption algorithms based on the factorization problem has been developed, enabling the detection of secret keys with a step size of $l/2$ under the condition $|p-q| \leq 2\hat{}(l/4)$ in an l-bit RSA modulus, and based on this method, a corresponding algorithm has been developed.

Implementation of the research results. Based on the scientific results obtained in the research work on the topic “Evaluation methods and algorithms for symmetric and public-key encryption algorithms”:

the method for evaluating nonlinear transformations of symmetric encryption algorithms, which enables the determination of encryption keys based on the order of repetition of joint occurrences of input bits at the output of nonlinear transformations and serves as an additional requirement to existing general cryptographic criteria in the evaluation of S-box transformations, was applied in the analysis and evaluation of the S-box of the SM4 symmetric encryption algorithm within the framework of the natural sciences project No. JSKY2021098 of Jining Normal University entitled “Research on the SM4 Algorithm” (certificate of Jining Normal University dated 15.10.2025 No. 20251015-001), as a result of which, in

evaluating the S-box transformation of the SM4 algorithm based on the NCOB property, deviations (outliers) were identified, in particular it was established that for input bit values of the 0th and 2nd positions (1,0), the number of joint occurrences of output bits at the 0th and 2nd positions with values (0,1) equals 10, whereas for the same input bit values (1,0), the number of joint occurrences of output bits at the 0th and 2nd positions with values (1,1) equals 24, and the obtained results made it possible to predict the corresponding bits of the last-round key with an accuracy of up to 75%;

the method developed on the basis of the Toom–Cook multiplication method, enabling factorization of an l-bit modulus of the RSA cryptosystem with sufficient memory of order $2^{\frac{l}{2}-2}$, was used in foreign publications (Journal of Machine and Computing, 05(03), 2025, pp. 1944–1957; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp. 842–862; Symmetry, 16, 2024, ID 764) in conducting a comprehensive analysis of the efficiency of Shor's algorithm using simulated quantum backends provided by the Qiskit platform, as a result of which a flexible and general implementation of integer factorization was proposed that allows dynamic input of numbers to be factorized, selection of random coprime numbers, and automatic generation of quantum circuits;

the method for evaluating nonlinear transformations of symmetric encryption algorithms based on the analysis of the repetition order of joint combinations of input bits at the output and enabling the determination of encryption keys, as well as the algorithms for determining encryption keys developed on its basis, were used in foreign publications (Discover Internet of Things, 5, 2025, pp. 1–20; Multimedia Tools and Applications, 8, 2024, pp. 24859–24886; Mesopotamian Journal of CyberSecurity, 5(2), 2025, pp. 842–862) in the development of high-performance and robust security systems for data transmission, formulation of recommendations for optimal requirements and a mathematical model of connectivity based on IoT parameters and NIST cryptographic standards, as well as in the advancement of cryptographic protocols through the application of encryption and decryption methods based on graph theory, as a result of which it was shown that the algorithm developed using the proposed method and algorithms outperforms the traditional Trivium approach, reducing encryption and decryption time in a ratio of 1:24, making it suitable for high-speed security requirements, while also demonstrating the adaptability of solutions for lightweight IoT infrastructures, and the application of Cartesian product graphs and complete bipartite graphs improves data confidentiality and integrity in communication systems;

the method for evaluating nonlinear transformations of symmetric encryption algorithms based on the analysis of the repetition order of joint combinations of input bits at the output and enabling the determination of encryption keys was used within the framework of the project "Development of a cloud-based electronic digital signature service" in generating parameters of digital signature algorithms and evaluating the strength of cryptographic algorithms (certificate of LLC "UNICON.UZ", Center for Scientific-Technical and Marketing Research, dated 29.01.2026 No. 7-2/211), as a result of which the interval partitioning method for

determining secret keys for encryption algorithms based on the factorization problem made it possible to systematically evaluate them during the generation of cryptographically strong keys, while the new method for evaluating nonlinear transformations of symmetric encryption algorithms, referred to as the “number of co-occurrences of bits,” enabled the assessment of the strength of cryptographic algorithms.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, five chapters, conclusion, references and appendices. The length of the dissertation is 153 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I Bo‘lim (Часть I; Part I)

1. Boykuziev Ilkhom, Angshuman Kh., Rupayan D., Abdurakhimov B., A Novel Approach to Integer Factorization: A Paradigm in Cryptography, Journal of “Concurrency and Computation: Practice and Experience”. Vol. 37, Issue 3, 2025. 37:e8365, © 2025 John Wiley & Sons Ltd., -13p. https://doi.org/10.1002/cpe.8365. (№3; Scopus Q1, IF = 0.437)
2. Rupayan Das,· Angshuman Khan, Rajeev Arya,·Boykuziev Ilkhom, Abdurakhimov Bakhtiyor, Nuriddin Safoyev, Zarif Khudoykulov, SSKA: secure symmetric encryption exploiting Kuznyechik algorithm for trustworthy communication, International Journal of System Assurance Engineering and Management (June 2024) 15(6):2391–2400 https://doi.org/10.1007/s13198-024-02253-7. (№3; Scopus Q2, IF = 0.377)
3. Boykuziev Ilkhom, Angshuman Kh., Abdurakhimov B., Rupayan D., Khudoykulov Z., Integral cryptanalysis: a new key determination technique for 3-phase Kuznyechik encryption, Journal of “Engineering Research Express”. №5 (2023). 035018, © 2023 IOP Publishing Ltd. -11p. https://doi:10.1088/2631-8695/ace58f. (№3; Scopus, IF = 0.351)
4. Abdurazzokov J., Abdurakhimov B., Boykuziev I., Allanov O. Algorithm for Generating Robust S-Boxes Using Adjacency Matrix Parameters // 2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). – IEEE. – 2023. – Pp. 372–377. – https://doi:10.1109/EECSI59885. 2023.10295947. (№3; Scopus, IF = 0.176)
5. Abdurakhimov B., Boykuziev I., Abdurazzokov J., Allanov O. Using the Capabilities of Artificial Neural Networks in the Cryptanalysis of Symmetric Lightweight Block Ciphers // Lecture Notes in Networks and Systems. – 2024. – Pp. 113–121. – https://doi:10.1007/978-3-031-51521-7_16. (№3; Scopus, IF = 0.166)
6. Jurayev Gayrat Umarovich, Bozorov Askar Xaitmurotovich, and Boykuziyev I.M., “Round key formation algorithm for symmetric block encryption algorithms”, E3S Web of Conferences 501, 02007 (2024) https://doi.org/10.1051/e3sconf/202450102007. (№3; Scopus, IF = 0.205)
7. Abdurakhimov B., Allanov O., Boykuziev I., Abdurazzokov J. Application of Artificial Neural Networks in the Classification of Classical Encryption Algorithms // 2022 International Conference on Information Science and Communications Technologies (ICISCT). – 2022. – Pp. 1–5. – https://doi:10.1109/ICISCT55600. 2022.10146796. (№3; Scopus)
8. Ilkhom Rakhmatullayev, Ilkhom Boykuziev, Analysis of cryptanalysis methods applied to stream encryption algorithms, Artificial Intelligence, Blockchain, Computing and Security, November 2023, Volume 1, https://doi:10.1201/9781003393580-60. (№3; Scopus)

9. Islambek Saymanov, Iouliia Skliarova, Ilkhom Boykuziev, and Orif Allanov, Introduction to Cryptographyfor Blockchain, In book: Fostering Machine Learning and IoT for Blockchain Technology Smart Cities Applications, Volume 1Publisher: Springer, Transactions on Computer Systems and Networks, https://doi:10.1007/978-981-96-4078-2. (№11; Springer)

10. Boyquziyev Ilxom Mardanoqulovich, Abduraximov Baxtiyor Fayziyevich, “Shifrlash algoritmlarining S-blok akslantirishlarini baholashdagi chiquvchi bitlarning birgalikda paydo bo‘lish xususiyatlari” Axborot xavfsizligi muammolari Ilmiy-amaliy va axborot-tahliliy jurnali, 1(1) 2024, B. 3-18. (01.00.00; OAK Rayosatining 2024-yil 30-noyabrdagi 1099-son qarori)

11. Boyquziyev Ilxom Mardanoqulovich, Abduraximov Baxtiyor Fayziyevich, Rahmatullayev Ilhom Raxmatullayevich, “Sonni tub ko‘paytuvchilarga ajratish algoritmining qo‘llanilishi” Axborot xavfsizligi muammolari Ilmiy-amaliy va axborot-tahliliy jurnali, 1(2) 2025, B. 24-38. (01.00.00; OAK Rayosatining 2024-yil 30-noyabrdagi 1099-son qarori)

12. Boyquziyev Ilxom Mardanoqulovich, “RSA kalitlarida tub sonlar farqi kichik bo‘lganda tezkor faktorizatsiya algoritmi” Axborot xavfsizligi muammolari Ilmiy-amaliy va axborot-tahliliy jurnali, 3(4) 2025, B. 45-57. (01.00.00; OAK Rayosatining 2024-yil 30-noyabrdagi 1099-son qarori)

13. Boykuziev Ilkhom Mardanokulovich, Genetic Algorithm Optimization Of Neural Network Hyperparameters For Predicting Key Bits In The S-Aes Cipher, American Journal of Applied Science and Technology, Vol.05 Issue 12 2025, -P. 106-112, doi:10.37547/ajast/Volume05Issue12-17. (№ 35, CrossRef)

14. Boykuziev Ilkhom Mardanokulovich, Classification Of Symmetric Encryption Key Bits Using Artificial Neural Networks, American Journal of Applied Science and Technology, Vol.05 Issue 12 2025, -P. 170-174, doi: https://doi.org/10.37547/ajast/Volume05Issue12-30. (№ 35, CrossRef)

15. Abduraximov B.F., Abdurazzoqov J.R., Boyquziyev I.M., S-AES RAUND kalitlari kriptotahliliga SVM giperparametrlarini optimallashtirish orqali tasniflash yondashuvi, “O‘zbekiston Milliy Axborot agentligi UZA Ilm-fan bo‘limi, Elektron Jurnal”. №11(73). 2025. -B.221-229. (05.00.00; OAK Rayosatining 2019 yil 28 martdagi 263/7.1-son qarori)

16. I.M. Boyquziev, I.R. Rakhmatullaev, “Sonlarni ko‘paytirish qoidasiga asoslangan faktorizatsiyalash algoritmi”, Harbiy aloqa va AKT xabarlari ilmiy uslubiy jurnali. 1(17) 2024. (OAK rayosatining 10.12.2019 yildagi № 272/7.2 sonli qarori bilan chop etishga ruxsat etilgan yopiq ilmiy ishlar ro‘yxatiga kiritilgan)

17. Ilxom Boyquziyev, Ilhom Rahmatullayev, O‘g‘iloy Axadova, “RSA shifrlash algoritmining maxfiy kalitini aniqlash algoritmi” Muhammad al-xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali. “Al-Farg‘oniy avlodlari”, (2)2024, B. 61–67. https://doi.org/10.5281/zenodo.11474014. (05.00.00; OAK rayosatining 2023-yil 30-sentyabrdagi 343-son qarori)

18. Abduraximov Baxtiyor Fayziyevich, Boyquziyev Ilxom Mardanoqulovich, Axadova O‘g‘iloy Chorshanbi qizi, “Faktorizatsiyalash muammosini bartaraf etuvchi algoritmlar tahlili”, Raqamli Transformatsiya va Sun’iy Intellekt ilmiy

jurnali VOLUME 2, ISSUE 4, AUGUST 2024, B. 100-106. (05.00.00; OAK Rayosatining 2023 yil 4 iyuldagi 340/5-son qarori)

19. Toshboyeva Feruza To‘lqin qizi, Abduraximov Baxtiyor Fayziyevich, Boyquziyev Ilxom Mardanoqulovich, “Elliptik egri chiziqlarning kriptografiyada qo‘llanilishi”, “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali, 1 (2) 2025, -B. 61-65. (05.00.00; OAK rayosatining 2023-yil 30-sentyabrdagi 343-son qarori)

20. Boyquziyev I., Saydullayev E., Rahmatullayev I., Elliptik egri chiziqlarning kriptografiyada qo‘llanilishi. Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali, 2(1)2024, -B. 71–76. (05.00.00; OAK Rayosatining 2023 yil 4 iyuldagi 340/5-son qarori)

II Bo‘lim (Часть II; Part II)

21. Ilkhom Rakhmatullayev, Ilkhom Boykuziev, Analysis of cryptanalysis methods applied to stream encryption algorithms, Proceedings of the International Conference on “Artificial Intelligence, Blockchain, Computing and Security (ICABCS 2023)”. Vol. 1. Gr. Noida, Up, India-2023. –P. 393-401 https://doi:10.1201/9781003393580-60. (№3; Scopus)

22. Boykuziev Ilkhom Mardanokulovich, Classification of S-AES encryption key bits using multilayer neural networks, “The latest pedagogical and psychological innovations in education”. Collection of scientific papers on materials of the international scientific-practical conference 09.12.2025, Pub. "ICP", London, Great Britain, –P. 75-78.

23. Boyquziyev Ilxom Mardanoqulovich, Kvant hisoblashning asoslari, “Zamonaviy axborot, kommunikatsiya texnologiyalari va AT-ta’lim tatbiqi muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Samarqand-2023. –B. 169-170

24. Boyquziyev Ilxom Mardanoqulovich, Kvant hisoblashning amaliyotda qo‘llanilishi, “Zamonaviy axborot, kommunikatsiya texnologiyalari va AT-ta’lim tatbiqi muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Samarqand-2023. –B. 170-172

25. Boyquziyev Ilxom Mardanoqulovich, Kvant hisoblashning kriptografiyada qo‘llanilishi, “Zamonaviy axborot, kommunikatsiya texnologiyalari va AT-ta’lim tatbiqi muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Samarqand-2023. –B. 172-173

26. Boyquziyev Ilxom Mardanoqulovich, “S-box akslantirishini baholashning chiquvchi bitlarning birgalikda paydo bo‘lishlari soni xususiyati”, Kiberxavfsizlikning yangi paradigmalari: global tahdidlar va mahalliy himoya strategiyalari Respublika ilmiy-nazariy konferensiyasi maqolalar to‘plami I-qism. Axborot – kommunikatsiya texnologiyalari va aloqa harbiy instituti, 2025-yil 12-fevral, -B. 149-154

27. Boyquziyev Ilxom Mardanoqulovich, Murodov Ma’murjon Ma’rupovich, “Sonlarni faktorlashning yangi algoritmi”, Kiberxavfsizlikning yangi paradigmalari: global tahdidlar va mahalliy himoya strategiyalari Respublika ilmiy-nazariy konferensiyasi maqolalar to‘plami I-qism. Axborot – kommunikatsiya texnologiyalari va aloqa harbiy instituti, 2025-yil 12-fevral, -B. 154-160

28. Boyquziyev Ilxom Mardanoqulovich, Yuldasheva Nafisa Salimovna,

“RSA algoritmining maxfiy kalitini aniqlashning yangi algoritmi”, Kiberxavfsizlikning yangi paradigmalari: global tahdidlar va mahalliy himoya strategiyalari Respublika ilmiy-nazariy konferensiyasi maqolalar to‘plami I-qism. Axborot – kommunikatsiya texnologiyalari va aloqa harbiy instituti, 2025-yil 12-fevral, -B. 160-144

29. Boykuziev Ilkhom Mardanokulovich, Genetic algorithm optimization of neural network hyperparameters for predicting key bits in the S-AES cipher, “The latest pedagogical and psychological innovations in education”. International online conference. Vol. 2 No. 12 (2025). 11.12.2025, www.incorp.org, Universitas Airlangga, Indonesia, -P. 88-91.

30. Rahmatullayev Ilhom Raxmatullayevich, Boyquziyev Ilxom Mardanoqulovich, “Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo‘llanish asoslari”, Kiberxavfsizlikning yangi paradigmalari: global tahdidlar va mahalliy himoya strategiyalari Respublika ilmiy-nazariy konferensiyasi maqolalar to‘plami I-qism. Axborot – kommunikatsiya texnologiyalari va aloqa harbiy instituti, 2025-yil 12-fevral, -B. 28-35

31. Abduraximov Baxtiyor Fayziyevich, Boyquziyev Ilxom Mardanoqulovich, Jo‘rayev Elmurod Xo‘shmurodovich, “Kriptografiyada matritsali akslantirishlarning qo‘llanilishi”, Harbiy-akademik litsey o‘quvchilarini vatanparvarlik ruhida tarbiyalashning milliy aspektlarini yaratish va zamonaviy ta’lim tarbiya tendensiyalarini tatbiq etish Respublika ilmiy-amaliy konferensiya maqolalari, Termiz 2025-yil 18-aprel, -B. 230-233.

32. Abduraximov Baxtiyor Fayziyevich, Boyquziyev Ilxom Mardanoqulovich, Noraliyev Sanjarbek Nurislom o‘g‘li, “Matematik akslantirishlarning kriptologiyada qo‘llanilishi”, Harbiy-akademik litsey o‘quvchilarini vatanparvarlik ruhida tarbiyalashning milliy aspektlarini yaratish va zamonaviy ta’lim tarbiya tendensiyalarini tatbiq etish Respublika ilmiy-amaliy konferensiya maqolalari, Termiz 2025-yil 18-aprel, -B. 234-236.

33. Boykuziev I.M., Rakhmatullaev I.R., E.I. Saydullayev, “Elliptik egri chiziqlarning kriptografiyada qo‘llanishi”, “IT-Xavfsizlik qalqoni. Harbiy sohaga axborot texnologiyalarini integratsiya qilishdagi muammo va yechimlar”. Respublika ilmiy-amaliy konferensiyasi maqolalar to‘plami. 2024-yil 17-mart. –B. 79-82 – ilmiy tezis.

34. Boyquziyev Ilxom Mardanoqulovich, “Sonlarni ko‘paytirishning Karatsuba usuliga asoslangan faktorizatsiyalash algoritmi”, “Ta’lim jarayoniga raqamli texnologiyalar va sun’iy intellektni joriy etish istiqbollari” mavzusida resublika ilmiy-amaliy konferensiya. Termiz davlat universiteti, 2024 yil 7-iyun – B. 310-314 – ilmiy tezis.

35. Boyquziyev Ilxom Mardanoqulovich, Ergashev Isroilbek Abdirashid o‘g‘li, Murodov Ma’murjon Ma’rupovich, “Faktorlash murakkabligiga asoslangan RSA asimmetrik shifrlash algoritmining murakkabligi tahlili”, “Ta’lim jarayoniga raqamli texnologiyalar va sun’iy intellektni joriy etish istiqbollari” mavzusida resublika ilmiy-amaliy konferensiya. Termiz davlat universiteti, 2024 yil 7-iyun – B. 302-306 – ilmiy tezis.

36. Boyquziyev Ilxom Mardanoqulovich, Axadova O‘g‘iloy Chorshanbi qizi, “Asimmetrik shifrlash algoritmlarining ishonchliligi”, “Ta’lim jarayoniga raqamli texnologiyalar va sun’iy intellektni joriy etish istiqbollari” mavzusida resublika ilmiy-amaliy konferensiya. Termiz davlat universiteti, 2024 yil 7-iyun –B. 299-301 – ilmiy tezis.

37. Boyquziyev Ilxom Mardanoqulovich, “Kiritilgan o‘lchamdagi tub sonlarni generatsiya qilishning Python dasturlash tilidagi dasturiy ta’minoti”, O‘zbekiston Respublikasi Adliya vazirligining elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi № DGU 35884, 05.04.2024

38. Boyquziyev Ilxom Mardanoqulovich, Allanov Orif Menglimuratovich, “Python dasturlash tilida yozilgan kiritilgan oraliqdagi tub sonlarni generatsiya qilib beruvchi dastur kodi”, O‘zbekiston Respublikasi Adliya vazirligining elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi № DGU 38163, 17.05.2024

39. Yuldasheva N.S., Boyquziyev I. M., Fayziyeva D.S., “Trigrammali kriptotahlilning Python dasturlash tilidagi realizatsiyasi”, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 42324, 07.09.2024.

40. Boyquziyev Ilxom Mardanoqulovich, Abduraximov Baxtiyor Fayziyevich, “S_boxning chiqish bitlarning birgalikda kelishlari sonini aniqlash dasturi”, O‘zbekiston Respublikasi Adliya vazirligining elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi № DGU 45585, 14.12.2024

41. Boyquziyev Ilxom Mardanoqulovich, Abduraximov Baxtiyor Fayziyevich, “Sonlarni ko‘paytirish qoidasiga asoslangan faktorlash algoritmi dasturi”, O‘zbekiston Respublikasi Adliya vazirligining elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi № DGU 45992, 19.12.2024

42. Boyquziyev Ilxom Mardanoqulovich, Abduraximov Baxtiyor Fayziyevich, “RSA asimmetrik shifrlash algoritmining maxfiy kalitini aniqlashning yangi usuli asosida ishlab chiqilgan algoritmning dasturi”, O‘zbekiston Respublikasi Adliya vazirligining elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi № DGU 45993, 19.12.2024

43. Boyquziyev Ilxom Mardanoqulovich, Allanov Orif Menglimuratovich, Murodov Ma’murjon Ma’rupovich, “Bigrammali kriptotahlilning Python dasturlash tilida amalga oshirilishi”. O‘zbekiston Respublikasining «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma‘lumotlar bazalarining huquqiy himoyasi to‘g‘risida»gi qonuniga asosan quyidagi elektron hisoblash mashinalari uchun yaratilgan dasturga berilgan guvohnoma. № DGU 42325, 13.09.2024.

Avtoreferat “Public Publish Printing” nashriyotida tahrirdan o‘tkazilib, o‘zbek, rus va ingliz tillarida matnlar o‘zaro muvofiqlashtirildi.

Bosishga ruxsat etildi: 06.04.2026-yil
Bichimi 60x84 $^{1}/_{16}$, “Times New Roman” garniturada raqamli bosma usulida bosildi.
Shartli bosma tabog‘i 4,0. Adadi: 100. Buyurtma: №25.

«Public Publish Printing» MChJ bosmaxonasida chop etildi.
Toshkent, M.Ulug‘bek tum., Moylisoy, 22.