“TOSHKENT IRRIGATSIYA VA QISHLOQ XO‘JALIGINI MEXANIZATSIYALASH MUHANDISLARI INSTITUTI” MILLIY TADQIQOT UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/26.05.2022.T.10.05 RAQAMLI ILMIY KENGASH

RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKTNI RIVOJLANTIRISH ILMIY-TADQIQOT INSTITUTI

ABDURAZZOQOV JAVOHIR RUSTAMOVICH

NOCHIZIQLI KOMPONENTLARNI SHAKLLANTIRISH VA TASNIFLASH ALGORITMLARI

05.01.03 – “Informatikaning nazariy asoslari”

texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi
AVTOREFERATI

Toshkent-2024

UDK: 004.853:004.421.5/.6

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

Contents of dissertation abstract of the doctor of philosophy (PhD) on technical sciences

“TOSHKENT IRRIGATSIYA VA QISHLOQ XO‘JALIGINI MEXANIZATSIYALASH MUHANDISLARI INSTITUTI” MILLIY TADQIQOT UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/26.05.2022.T.10.05 RAQAMLI ILMIY KENGASH

RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKTNI RIVOJLANTIRISH ILMIY-TADQIQOT INSTITUTI

ABDURAZZOQOV JAVOHIR RUSTAMOVICH

NOCHIZIQLI KOMPONENTLARNI SHAKLLANTIRISH VA TASNIFLASH ALGORITMLARI

05.01.03 – “Informatikaning nazariy asoslari”

texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi
AVTOREFERATI

Toshkent-2024

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2024.1.PhD/T4410 raqam bilan ro‘yxatga olingan.

Dissertatsiya Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot institutida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezume)) Ilmiy kengash veb-sahifasida (www.tiiame.uz) va “Ziyonet” Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Abduraximov Baxtiyor Fayziyevich** fizika-matematika fanlari doktori, professor
Rasmiy opponentlar:	**Mirzayev Nomaz** texnika fanlari doktori, professor
	Xodiyev Shuxrat Ilxamovich texnika fanlari nomzodi, dotsent
Yetakchi tashkilot:	**Sharof Rashidov nomidagi Samarqand davlat universiteti**

Dissertatsiya himoyasi Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti Milliy tadqiqot universiteti huzuridagi DSc.03/26.05.2022.T.10.05 raqamli Ilmiy kengashning 2024-yil «22» noyabr soat 1400 dagi majlisida bo‘lib o‘tadi (Manzil: 100095, Toshkent shahri, Qori Niyoziy ko‘chasi 39, Tel.: (+99871) 237-46-68; faks: (+99871) 237-19-36; e-mail: admin@tiiame.uz).

Dissertatsiya bilan “Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti” Milliy tadqiqot universitetining Axborot-resurs markazida tanishish mumkin (342-raqam bilan ro‘yxatga olingan). (Manzil: 100000, Toshkent shahri, Qori Niyoziy ko‘chasi, 39 uy. Tel.: (+99871) 237-19-45).

Dissertatsiya avtoreferati 2024-yil “12” 11 da tarqatildi.
(2024-yil “11” 11 dagi №7 raqamli reestr bayonnomasi.)

N.S. Mamatov
Ilmiy darajalar beruvchi
Ilmiy Kengash raisi,
texnika fanlari doktori, professor

D.Q. Bekmuratov
Ilmiy darajalar beruvchi
Ilmiy Kengash ilmiy kotibi,
texnika fanlari bo‘yicha falsafa doktori

S.S. Radjabov
Ilmiy darajalar beruvchi
Ilmiy Kengash qoshidagi
ilmiy seminar raisi,
texnika fanlari doktori, katta ilmiy xodim

KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahonda axborot texnologiyalarining rivojlanishi va keng ko‘lamli integratsiyasi ortidan, raqamli ma’lumotlar hajmining kattalashuvi hamda ularning xavfsizligi masalalari tobora murakkablashmoqda. Inson ishlov bera olmaydigan katta hajmdagi ma’lumotlarning paydo bo‘lishi ularni saqlash, ishlov berish, uzatish va xavfsizligida mashinali o‘qitish usullarini qo‘llash zaruratini keltirib chiqardi. Xususan, blokli simmetrik kalitli shifrlash algoritmlari, axborot xavfsizligining asosiy tayanchi bo‘lib, ularning samaradorligi va ishonchliligi kiber tahdidlarga qarshi muhim himoyani ta’minlaydi. Zamonaviy kiber hujumlarning murakkabligi va o‘zgaruvchanligi ushbu algoritmlarning doimiy takomillashuvi bilan bir qatorda ularda yangi innovatsion usullarni qo‘llashni talab qiladi. Blokli shifrlash algoritmlarini takomillashtirish masalalarini yechishda mashinali o‘qitish va evolyutsion algoritmlarni qo‘llash muhim tadqiqot yo‘nalishlaridan biri hisoblanadi. Mazkur masalalar bo‘yicha AQSH, Hindiston, Xitoy, Rossiya, Germaniya, Yaponiya va boshqa mamlakat olimlari mashinali o‘qitish va genetik algoritmlarni blokli shifrlashda qo‘llash orqali, uning nazariy va amaliy yechimlarini ishlab chiqishga e’tibor qaratmoqda.

Jahonda simmetrik kalitli algoritmlarning samaradorligini oshirish va yangi xavfsizlik tahdidlariga moslashuvchanlikni ta’minlash zaruratini hisobga olgan holda, sohaga sun’iy intellekt va genetik algoritmlarni qo‘llash bo‘yicha muhim tadqiqotlar olib borilmoqda. Ushbu tadqiqotlar, simmetrik shifrlash jarayonlarini optimallashtirish, nochiziqligi yuqori komponentlarni shakllantirish, kalitlarni boshqarish va turli hujumlarga bardoshlilikni oshirish orqali axborot xavfsizligini talabini yanada yaxshilashni maqsad qiladi. Shu bilan birga zamonaviy shifrlash algoritmlarni ishlab chiqish bilan bir qatorda ularning ishonchliligini baholash va zaifliklarini aniqlash muhimdir. Bu sohalarni integratsiyalashda shifrlash algoritmlarining kalit bitlarini to‘g‘ri tasniflash uchun mos o‘quv tanlanmani shakllantirish, mashinali o‘qitish usuli va uning giperparametrlarini optimallashtirish muhim ahamiyatga ega. Shifrlash algoritmlari bardoshligini oshirish uchun ichki nochiziqli komponentlarni shakllantirishda foydalanilayotgan funksiyalarni to‘g‘ri tanlash, qiymatlarning yaroqliligini baholash va evolyutsion algoritmlarni qo‘llash muhim vazifalardan biri hisoblanadi.

Respublikamizda axborot-kommunikatsiya texnologiyalarining barcha iqtisodiy va ijtimoiy sohalarga joriy etilishi, zamonaviy taraqqiyotning asosiy yo‘nalishlaridan biri hisoblanadi. «Raqamli O‘zbekiston – 2030» strategiyasida «…iqtisodiyot tarmoqlarida sun’iy intellekt, kriptografiya, mashinali o‘qitish imkoniyatlarini o‘rganish va ularni amaliyotga tatbiq etish...», «...infratuzilmalarning axborot xavfsizligini va hujjatlarning himoyasini ta’minlash...», «... davlat organlari, jismoniy va yuridik shaxslar uchun axborotni himoya qilish ....»[1] hamda Respublikamizda kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risidagi Qarorda «…

[1] O‘zbekiston Respublikasi Prezidentining, 2020-yil 5-oktyabr PF-6079-sonli “Raqamli O‘zbekiston — 2030” strategiyasini samarali amalga oshirish chora-tadbirlari to‘g‘risidagi Farmoni.

sohadagi ilmiy-tadqiqotlar ko‘lami va amaliy ahamiyatini oshirish...»[2] hamda zamonaviy kriptotahlil usullarini yaratish bo‘yicha vazifalar belgilangan. Mazkur vazifalarni amalga oshirishda jumladan, axborot himoyasida muhim o‘rin tutuvchi simmetrik kalitli shifrlash algoritmlarini mashinaviy o‘qitish va genetik algoritmlar asosida takomillashtirish hamda zamonaviy kriptotahlillarga baholash muhim vazifalardan biri hisoblanadi. Prezidentimizning 2020-yil 28-apreldagi PQ-4699-son «Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora tadbirlari to‘g‘risida», 2021-yil 17-fevraldagi PQ-4996-son «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida»gi Qarorlari hamda sohaga oid boshqa me’yoriy-huquqiy hujjatlarda 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-kommunikasiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Mashinali o‘qitish usullari va genetik algoritmlarni, simmetrik kalitli shifrlash algoritmlarining nochiziqli komponentlarini tasniflash va shakllantirish masalalari bo‘yicha N.Kopal, R.Rivest, L.Lerman, A.Benamira, M.Perusheska, Y.Alsariera, A.Petrov, H.Kim, X.Yin, W.Zhang, A.Zahid, A.Ko‘kcham, S.Omran, Y.Wang, va boshqa olimlar tomonidan izlanishlar olib borilmoqda.

Respublikamizda mashinali o‘qitish usullari va genetik algoritmlarni nochiziq ma’lumotlarni tasniflash hamda turli masalalarda optimal yechimlarni qo‘llashning nazariy asoslarini yaratishga va amaliy tadbiqlarini rivojlantirishga T.F.Bekmuratov, M.M.Kamilov, Sh.X.Fozilov, D.T.Muxamediyeva, F.T.Adilova, R.X.Xamdamov, N.A.Ignatyev, N.S.Mamatov, X.A.Primova, S.S.Rajabov va boshqalar o‘zlarining katta hissalarini qo‘shganlar. Shifrlash algoritmlari va ularning kriptografik nochiziqli komponentlarni shakllantirish hamda bardoshligini baholash masalalariga M.Aripov, P.F.Xasanov, S.K.Ganiyev, B.F.Abduraximov, M.M.Karimov, D.Y.Akbarov, G.U.Jurayev, G‘.N.Tuychiyev, D.M.Kuryazov, A.B.Sattarov va boshqalar boshchiligidagi ilmiy jamoalarning ishlari bag‘ishlangan.

Shu bilan bir qatorda mashinali o‘qitish usullari va genetik algoritmlar, simmetrik kalitli shifrlash algoritmlarining nochiziqli komponentlarini tasniflash va shakllantirish masalalarida qo‘llashga yetarlicha e’tibor qaratilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim va ilmiy tadqiqot muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti ilmiy-tadqiqot ishlari rejasining FZ-20200929308 “Axborot xavfsizligini ta’minlash tizimlarida foydalanuvchilarni biometrik avtorizatsiyalashning integrallashgan texnologiyalari nazariy asoslarini yaratish” (2021-2023) raqamli fundamental tadqiqotlar loyihasi doirasida bajarilgan.

[2] O‘zbekiston Respublikasi Prezidentining, 2024-yil 15-avgustdagi PQ-293-sonli “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori.

Tadqiqotning maqsadi mashinali o‘qitish va genetik algoritm yordamida simmetrik blokli shifrlarning nochiziqligi yuqori komponentlarini tasniflash va shakllantirish algoritmlarini ishlab chiqish.

Tadqiqotning vazifalari:

mashinali o‘qitish usullari va genetik algoritmlarni shifrlash algoritmlari nochiziq komponentlariga qo‘llash bo‘yicha zamonaviy yondashuvlarni tahlil qilish;

simmetrik shifrlash algoritmlari nochiziq komponentlari asosida o‘quv va nazorat tanlanmalarni shakllantirish yondashuvni ishlab chiqish;

tayanch vektorlar usuli giperparametrlarini optimallashtirish asosida raund kalitlarini tasniflash aniqligini oshirish yondashuvini shakllantirish;

genetik algoritmni neyron tarmoq arxitekturasida qo‘llash asosida shifrlash kaliti bitlarini tasniflash algoritmini ishlab chiqish;

xosmas qo‘shnilik matritsani genetik algoritm yordamida ajratish va affin funksiyada qo‘llash asosida statik nochiziq komponent qiymatlarini shakllantirish algoritmi ishlab chiqish;

genetik algoritm parametrlarida kriptografik baholashni inobatga olgan holda dinamik nochiziq komponentlar qiymatlarini shakllantirish algoritmi ishlab chiqish.

nochiziqligi yuqori komponentlarini shakllantirish dasturiy majmuasini ishlab chiqish va hisoblash eksperimentlarini o‘tkazish.

Tadqiqotning obyekti simmetrik blokli shifrlash algoritmlarining nochiziq komponentlarini tasniflash va shakllantirish jarayonlari olingan.

Tadqiqotning predmetini mashinali o‘qitish usullarini simmetrik shifrlash algoritmining kalitlarini tasniflashda qo‘llash, nochiziq almashtirish komponenti (S-komponent)ning yuqori bardoshliligini ta’minlovchi statik va dinamik qiymatlarni shakllantirish algoritmi va dasturiy ta’minoti tashkil etadi.

Tadqiqotning usullari. Ishning nazariy tadqiqotlari matematik tahlil, diskret matematika, ehtimollar nazariyasi va matematik statistika, hisoblash matematikasi, amaliy kriptografiya va kriptotahlil usullariga asoslangan holda amalga oshirilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

simmetrik shifrlash algoritmlari nochiziq komponentlari asosida o‘quv va nazorat tanlanmalarni shakllantirish yondashuvi taklif etilgan;

tayanch vektorlar usuli giperparametrlarini optimallashtirish asosida raund kalitlarini tasniflash aniqligini oshirish yondashuvi taklif etilgan;

genetik algoritmni neyron tarmoq arxitekturasida qo‘llash asosida shifrlash kaliti bitlarini tasniflash algoritmi ishlab chiqilgan;

xosmas qo‘shnilik matritsani genetik algoritm yordamida ajratish va affin funksiyada qo‘llash asosida statik nochiziq komponent qiymatlarini shakllantirish algoritmi ishlab chiqilgan;

genetik algoritm parametrlarida kriptografik baholashni inobatga olgan holda dinamik nochiziq komponentlar qiymatlarini shakllantirish algoritmi ishlab chiqilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

nochiziq ma’lumotlarni tasniflash aniqligini oshirish uchun mashinali o‘qitish usullari giperparametrlarni tanlash algoritmi ishlab chiqilgan;

giperparametrlarni tanlash algoritmi simmetrik kalitli blokli shifrlash algoritmi kalit bitlarini tasniflashga qo‘llanilgan;

statik 256 qiymatli, yuqori bardoshli nochiziq almashtirish komponentini hosil qilish algoritmi ishlab chiqilgan;

genetik algoritm parametrlarida kriptografik baholashni inobatga olgan holda dinamik nochiziq komponentlar qiymatlarini hosil qiluvchi algoritm va dasturiy majmuasi ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi simmetrik shifrlash algoritmlarining nochiziq komponentlariga nisbatan masalaning korrekt qo‘yilishi hamda ishlab chiqilgan algoritmlarni real va tajribaviy natijalarining qiyosiy tahlili bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqotda olingan natijalarning ilmiy ahamiyati simmetrik blokli shifrlash algoritmining kalit bitlarini tasniflashda tayanch vektorlar usuli va neyron tarmoq giperparametrlari zamonaviy optimallashtirish usullari hamda genetik algoritm yordamida tanlanib, tasniflash aniqligi yaxshilangani bilan, nochiziqli S-komponentlarini shakllantirish algoritmlarining natijalarida yuqori bardoshlilikka erishganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati ishlab chiqilgan algoritmlar va dasturiy ta’minotni nochiziqli ma’lumotlarni tasniflash masalalarida va zamonaviy simmetrik blokli shifrlarning raund funksiyalarida qo‘llash mumkinligi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Tadqiqotda ishlab chiqilgan nochiziqli komponentlarni shakllantirish va tasniflash algoritmlari hamda dasturiy majmua asosida:

genetik algoritmga asoslangan neyron tarmoq giperparametrlarni optimallashtirish orqali ishlab chiqilgan tasniflash algoritmi Surxondaryo viloyati statistika boshqarmasining Raqamlashtirish va ma’lumotlarni saqlash markazida joriy etilgan (Surxondaryo viloyati hokimligining 2024-yil 23-sentabrdagi 07-07/1988-sonli ma’lumotnomasi). Natijada ishlab chiqilgan algoritm iqtisodiy ko‘rsatgichlar haqidagi ma’lumotlarni bashoratlash 8-10%ga yaxshilangan hamda 11-13% ga vaqtni qisqartirish imkonini bergan;

tadqiqotda genetik algoritmga asoslangan holda shakllantirilgan *S*-komponent AESning ichki nochiziq almashtirish bloki o‘rniga qo‘yish orqali yaratilgan dasturiy majmua, Raqamli texnologiyalar vazirligi Surxondaryo viloyat xududiy sho‘basida katta hajmdagi ma’lumotlarni shifrlash maqsadida joriy etilgan (Surxondaryo viloyati hokimligining 2024-yil 23-sentabrdagi 07-07/1988-sonli ma’lumotnomasi). Natijada tasodifiy yuz mingta ochiq matn va kalitlari kiritib, mavjud AES algoritmi bilan solishtirilganda vaqt sarfini 11,5-12,5% gacha ochiq matnlarni shifrlash hamda shifrni dastlabki matnga o‘girishda vaqtni 10,5%-12% gacha qisqartirish imkonini bergan;

tadqiqot ishida shakllantirilgan statik *S* nochiziq komponent simsiz lokal tarmoq xavfsizligini ta’minlash, ma’lumotlarni shifrlash jarayonidagi samaradorligini baholash maqsadida Surxondaryo viloyati Davlat aktivlarini boshqarish boshqarmasi tasischiligidagi “Axborot-kommunikatsiya texnologiyalarini rivojlantirish markazi” MCHJda axborot almashish jarayoniga

joriy etilgan (Surxondaryo viloyati hokimligining 2024-yil 23-sentabrdagi 07-07/1988-sonli ma’lumotnomasi). Natijada statik *S*-komponent umumiy bardoshlilik ko‘rsatgichi bo‘yicha AES shifrlash standartining ichki nochiziq almashtirish blokidan o‘rtacha 12,5% yuqori ko‘rsatgichga erishish imkonini bergan;

tadqiqotda shakllantirilgan *S*-komponent asosida ishlab chiqilgan dasturiy majmua katta hajmdagi ma’lumotlarni himoyalash maqsadida Surxondaryo viloyati IT park Termiz filialida joriy etilgan (Surxondaryo viloyati hokimligining 2024-yil 23-sentabrdagi 07-07/1988-sonli ma’lumotnomasi). Natijada majmuaga tasodifiy bir millionta ochiq matn va kalitlarni kiritish orqali hosil qilingan shifr matnlar AES algoritmi bilan taqqoslaganda vaqt sarfi bo‘yicha 13-15% ga qisqartirish imkonini bergan;

genetik algoritmga asoslangan shakllantirilgan statik *S*-komponent Xitoy davlatining SM4 shifrlash algoritmining *S*-komponenti o‘rniga qo‘yish orqali Xitoy davlatining Inner Mongolia Wangxin Information Security Service Co., Ltd tashkilotiga joriy etilgan (Inner Mongolia Wangxin Information Security Service Co. Ltd tashkilotining 2024-yil 10-apreldagi WXSEC20240410005 raqamli ma’lumotnomasi) Natijada SM4 shifrlash algoritmi bardoshligi o‘rtacha 13-13,5% yaxshilanishiga erishilgan.

Tadqiqot natijalarining approbatsiyasi. Mazkur tadqiqotning nazariy va amaliy natijalari 4 ta xalqaro va 5 ta respublika ilmiy-amaliy anjumanlarida ma’ruza qilingan va muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiya mavzusi bo‘yicha jami 21 ta ilmiy ish chop etilgan bo‘lib, shulardan, 9 tasi O‘zbekiston Respublikasi Oliy attestatsiya komissiyasi tomonidan tavsiya etilgan ilmiy nashrlarda, jumladan, 5 tasi xorijiy jurnallarda (4 ta maqola Scopus bazasiga indekslangan) va 4 tasi respublika jurnallarida chop etilgan hamda 3 ta EHM uchun yaratilgan dasturiy vositalarni qayd qilish guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiyaning hajmi 120 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zaruriyati asoslangan, tadqiqotning O‘zbekiston Respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, tadqiqot natijalarning ishonchliligi asoslab berilgan, ularning nazariy va amaliy ahamiyati, tadqiqot natijalarini amalda joriy qilish holati, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Nochiziqligi yuqori algoritmlar komponentlarni shakllantirish va tasniflash muammolari tahlili”** deb nomlangan birinchi bobida ma’lumotlarni intellektual tahlil qilish usullari va algoritmlari hamda simmetrik blokli shifrlash algoritmlarinining zamonaviy holati tahlil qilingan. Tasniflash masalasiga simmetrik kalitli algoritmning shifrlash va raund kalitlari qaralgan holda, ularni tasniflash muammolari aniqlangan. Blokli shifrlash algoritmlarida nochiziq *S*-

komponentlarini shakllantirish muammolari o‘rganilib, genetik algoritm yordamida yangi natija va algoritmlar ishlab chiqish bayon etilgan.

1.1. ma’lumotlarni intellektual tahlil qilish usullari va algoritmlariga bag‘ishlangan bo‘lib, tadqiqot uchun tayanch vektorlar usuli (SVM) va **s**un’iy **n**eyron **t**armoq (SNT) usullari tanlangan holda, ularning giperparametrlarini tanlash muammolari o‘rganilgan. Mazkur usullarning binar tasniflash masalalarida samarali natijalarga erishishi, shu bilan birga giperparametrlarini tanlash, yechim uchun muhim ahamiyatga ega jarayonligi keltirilgan.

1.2. paragrafda komponentlari nochiziq bo‘lishi talab etiluvchi algoritmlar va ularning tahlili bo‘yicha ma’lumotlar keltirilgan. Mazkur paragrafda zamonaviy blokli shifrlash algoritmlarining turlari ularning ma’lumotlarni himoyalashdagi o‘rni, ichki tuzilishi va nochiziq komponentlarining sharhi keltirilgan.

1.3 paragrafda nochiziq almashtirish komponentlarni baholash mezonlari tahlili qilingan. Kriptografik bardoshli *S*-komponentlarni shakllantirishning asosiy mezonlar sifatida nochiziqlik, differensial yaqinlashish ehtimolligi, qat’iy lavin samaradorlik, algebraik immuniteti, o‘zgarmas va qarama-qarshi o‘zgarmas qiymatlari tanlanib, mazkur mezonlarga baholash zarurati hamda ularning tavsiyaviy qiymatlari keltirilgan.

1.4. paragrafda nochiziq komponentlarni tasniflash va shakllantirish muammolari tahlil qilingan bo‘lib, simmetrik blokli shifrlarda mashinali o‘qitish algoritmlarining integratsiyasi, kriptografik xavfsizligi va samaradorligini oshirish yo‘llarni, shu masalalarga bag‘ishlangan tadqiqotlar haqida bayon etadi. Blokli shifrlash algoritmlarida bardoshli S-komponentni shakllantirish murakkab vazifa bo‘lib, genetik algoritmlar yordamida uni shakllantirish kriptografiyada yangi yondashuvlarni taqdim etmoqda. Bu usul komponentlarning nochiziqlik va boshqa kriptografik talablarga mosligini optimallashtirish imkonini beradi.

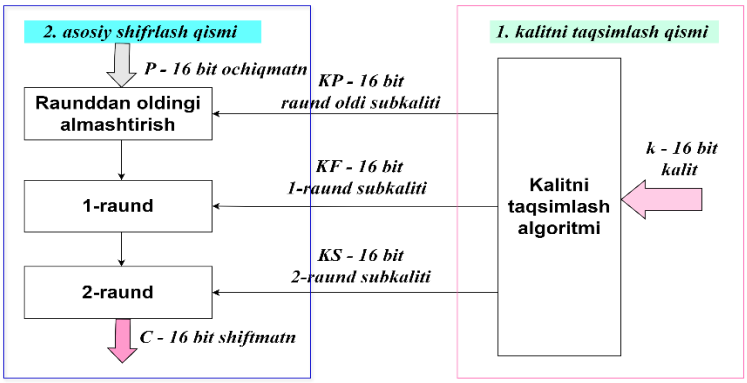
1.5 paragrafda dissertatsiya tadqiqoti maqsadiga erishish uchun hal qilinishi kerak bo‘lgan masalalar shakllantirilgan. Nochiziq komponentlar sifatida, simmetrik blokli shifrlash algoritmlarining kalit bitlari va nochiziq *S*-komponenti tanlab olindi, bunda tadqiqot muammolari quyidagicha qo‘yildi:

Tasniflash masalasi uchun ochiq matnlar to‘plami $\mathcal{P}=\{P_1,P_2,\ldots,P_i\}$, bu yerda har bir $P_i\in\{0,1\}^m$. Kalit bitlar to‘plami $\mathcal{K}=\{K_1,K_2,\ldots,K_i\}$, bu yerda har bir $K_i\in\{0,1\}^n$. $\mathcal{C}=\{C_1,C_2,\ldots,C_i\}$, bu yerda har bir $C_i\in\{0,1\}^m$. m – ochiq va shifr matn bitlari uzunligi, n – kalit bitlari uzunligi. Shifrlash funksiyasi $E:\mathcal{K}\times\mathcal{P}\to\mathcal{C}$ – bu yerda $E(K_i,P_i)=C_i$ bo‘lib K_i kaliti va P_i ochiq matn uchun C_i shifr matnni hosil qiladi. Berilgan (P_i,C_i) juftliklari asosida, shifrlashda foydalanilgan kalit K_i ni tasniflash uchun mashinali o‘qitish modelini ishlab chiqish kerak bo‘lsin. Shakllantirish lozim bo‘lgan nochiziq *S*-komponent simmetrik shifrlash algoritmlarining muhim qismi hisoblanib, nochiziqlik, qat’iy lavin samaradorlik ko‘rsatgichi, differensial yaqinlashish ehtimoli kichik, o‘zgarmas va qarama-qarshi o‘zgarmas qiymatlari soni ideal holatda 0 ga teng bo‘lishi maqsadga muvofiq. Mazkur mezonlarga mos keluvchi *S*-komponentlarni katta elementlar to‘plamidan turli baholash mezonlari asosida shakllantirish zarurati mavjudligini ko‘rsatadi.

Dissertatsiyaning **“Nochiziqligi yuqori komponentlarni tasniflash algoritmlari”** deb nomlangan ikkinchi bobi soddalashtirilgan simmetrik kalitli algoritmlarning raund va shifrlash kaliti bitlarini tasniflash usullari, shakllantirilgan nochiziq ma’lumotlarni o‘qitishga tayyorlash, SVM va SNT giperparametrlarni tanlash algoritmlarini ishlab chiqishga bag‘ishlangan.

2.1 paragrafda klassik shifrlash algoritmlari Affin, Vijener va Playferdan hosil qilingan shifr matnlar nochiziq ma’lumotlar sifatida olinib, ularning turini aniqlash uchun SNT dan foydalanilgan, tajriba davomida modelning o‘quv aniqligi 95% dan, nazorat aniqligi esa 79 %dan ortiq bo‘lishiga erishilgan. Ushbu natijalar mashinali o‘qitishni kriptotahlil muammolariga qo‘llash orqali yangi usul va natijalarni olish, zamonaviy blokli shifrlarni kriptotahlilida foydalanish mumkinligini ko‘rsatdi.

2.2 paragrafda simmetrik shifrlash algoritmi sifatida soddalashtirilgan S-AES algoritmi tanlab olinib, tasniflash masalasi uning shifrlash kaliti bitlarini aniqlashga qaratidi. Mashinali o‘qitish usullarining kirishi sifatida ochiq matn va shifr matn juftliklari qaraldi, chiqishi uchun kalit bitlari olinib tajribalar SNT usulida o‘tkazildi. Tadqiqotda S-AESning kalit bitlarini tasniflashda mashinali o‘qitish usuli bilan birga uning giperparametrlarini optimal tanlash muammosi mavjudligi aniqlandi.



1-rasm. O‘quv tanlanmalarni shakllantirishda tanlab olingan S-AES qismlari

2.3 paragrafda S-AESning kalit bitlarini tasniflash uchun, uning shifrlash raundlari va kalitlarni taqsimlash qismlari alohida 2 ta qismga bo‘lib olindi. 1-qism S-AES ning kalitni taqsimlash algoritmiga kiruvchi shifrlash kalit k bitlari va undan hosil bo‘luchi KP, KF, KS raund kalitlari o‘quv tanlanma sifatida tanlandi. 2-qism o‘quv tanlanmasi k shifrlash kalitni tasodifiy kiritib undan hosil bo‘lgan raund kalitlari bitlari KP, KF, KS lar tanlab olingan 2 ta p_1 = 1000100010001000 va p_2 = 1100110011001100 ochiq matnlar bilan c_1 va c_2 shifr matnlar hosil qilindi.

S-AES raund funksiyasida qo‘llanilgan S-komponent S_b={9,4,A,B,D,1,8,5,6,2,0,3,C,E,F,7} va c_1 va c_2 shifrlaring binar qiymatlari bilan birgalikda o‘quv tanlanmasi hosil qilindi. O‘quv tanlanma SVMga kiruvchi sifatida va raund kalitlarining har bir biti tasniflanuvchi sifatida qaralgan. Optuna dasturi yordamida $M=1000$ turli sinovlar orqali θ-giperparametrlari uchun optimal qiymatlar tanlandi. SVMning θ-giperparametrlar va ularning qidiruv maydoni C=[10^{-3}, 10^{3}], Y_t - yadro funksiyalari, chiziqli, ko‘phadli, radial asosli va sigmoidal yadro funksiyalari va ularga tegishli parametrlarni sonli oraliqlarda olindi. Natijada maksimal tasniflash aniqligi 88,46%, minimal tasniflash aniqligi 61,54% bo‘lib, o‘rtacha tasniflash aniqligi 70,67% ni tashkil etdi. Shifrlash kaliti bitlari uchun o‘quv tanlanmalarini

shakllantirishda 16 bitdan iborat *N=2048* ta tasodifiy *k* kalitlar tanlandi. *k* kalitlarni S-AESning kalitlarni taqsimlash qismiga kiritilib, raund funksiyalari subkalitlari *KP=16 bit, KF=16 bit, KS=16bit* lardan iborat 48 bitni tashkil qiluvchi to‘plam hosil qilindi. Raund kalitlari orqali shifrlash *k* ni tasniflash uchun S_K ko‘rinishidagi o‘quv tanlanma shakllandi. Hosil qilingan S_K o‘quv tanlanma SNT uchun x_n kiruvchi tasodifiy shifrlash kaliti *k* orqali generatsiya qilingan *kp*, *kf* va *ks* subkalit bitlaridir. Chiqish y_n sifatida har bir ustunidagi shifrlash *k* kalit bitini tasniflash uchun alohida o‘quv tanlanmalar yaratildi.

$$S_K = \begin{bmatrix} kp_{1,1} & kp_{1,2} & \cdots & kp_{1,n} & kf_{1,1} & kf_{1,2} & \cdots & kf_{1,n} & ks_{1,1} & ks_{1,2} & \cdots & ks_{1,n} & k_{1,1} & k_{1,2} & \cdots & k_{1,n} \\ kp_{2,1} & kp_{2,2} & \cdots & kp_{2,n} & kf_{2,1} & kf_{2,2} & \cdots & kf_{2,n} & ks_{2,1} & ks_{2,2} & \cdots & ks_{2,n} & k_{2,1} & k_{2,2} & \cdots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ kp_{N,1} & kp_{N,2} & \cdots & kp_{N,n} & kf_{N,1} & kf_{N,2} & \cdots & kf_{N,n} & ks_{N,1} & ks_{N,2} & \cdots & ks_{N,n} & k_{N,1} & k_{N,2} & \cdots & k_{N,n} \end{bmatrix}$$

SNTning giperparametrlarini tanlash va arxitekturasini qurishning **A1** genetik algoritmi quyidagi qadamlardan iborat:

Kiruvchi parametrlar va ularning qiymatlari: O‘quv tanlanma, neyron tarmoqning giperparametrlari va ularning sonli oraliqlari.

Chiquvchi natija: Berilgan o‘quv tanlanmaning tasniflanishi kerak bo‘lgan chiqish sinfiga eng yuqori nazorat tanlanmada aniqlangan giperparametrlar.

1-qadam. Barcha mumkin bo‘lgan giperparametrlar to‘plamini *H* bilan belgilaymiz. Har bir giperparametr $h_i \in H$ oldindan belgilangan giperparametr oraliq qiymatlarini qabul qiladi. Mazkur masala uchun quyidagicha belgilandi:
O‘rganish tezligi (*LR*): $LR \in \{0.001, 0.01, 0.1\}$, batch hajmi (*BS*): $BS \in \{16, 32, 64\}$, dropout darajasi (*DR*): $DR \in \{0.1, 0.2, 0.4, 0.5\}$, yo‘qotish funksiyasi (*LF*): $LF \in \{\text{MSE}\}$, qatlamlar soni (*LN*): $LN \in \{5, 6, 7, 8, 9\}$, aktivatsiya funksiyalari to‘plami *(AF)*: $AF \in \{"relu", "elu", "selu", "prelu", "gelu"\}$.

2-qadam. Boshlang‘ich P_0 populyatsiya *n* ta individlar bilan yaratiladi. $P_0 = \{I_1, I_2, \ldots, I_n\}$, bu yerda har bir I_n neyron tarmog‘ining giperparametrlar va qatlamlar sozlanmasidir.

$$I_n = \{LR_n, BS_n, DR_n, LF_n, LS_n\},\ LS_n = \{(NE_{n1}, AF_{n1}), \ldots, (NE_{nL}, AF_{nL})\},$$

bunda *LS* – qatlamlar soni, *NE* – neyron, *AF* – aktivatsiya funksiyasi, *L* – neyron tarmog‘i qatlamining umumiy sonini ifodalaydi. Bu parametrlar qiymati 1-qadamda berilgan giperparametrlarga tegishli to‘plamdan tasodifiy tanlanadi.

3-qadam. Har bir *I* - individning mosligi giperparametrlar asosida yaratilgan neyron tarmog‘i arxitekturasi nazorat to‘plamidagi aniqlikni *MSE* funksiyasi bilan aniqlash orqali yaroqliligi baholanadi. Bu ifoda quyidagicha ifodalaniladi:

$$f(I_n) = AC_{naz}(M_d(I_n)),$$

bu yerda $M_d(I_n)$, I_n - individining giperparametrlari asosida yaratilgan neyron tarmog‘ini bildiradi, va AC_{naz} nazorat to‘plamidagi aniqligini ifodalaydi.

4-qadam. Krossover operatori ikki I_p ota va I_q onadan krossover operatsiyasi orqali yangi avlod I_c yaratiladi. Bu operatsiya har bir giperparametr uchun quyidagicha amalga oshiriladi:

$$I_c[g]=\begin{cases} I_p[g] & \text{agar } t_s < 0.5 \\ I_q[g] & \text{aks holda} \end{cases},$$

bu yerda t_s – 0 dan 1 gacha bo‘lgan oraliqdan tasodifiy qiymat. g – gen bo‘lib, har bir giperparametrni ifodalovchi o‘zgaruvchidir.

5-qadam. Mutatsiya har bir tanlangan gen g uchun, mutatsiya $I_n[g]=g'$ning 1-qadamdagi oraliqlardan olingan tasodifiy qiymat. Tanlangan giperparametrga yangi qiymatni qo‘llagan holda faqat tanlangan giperparametr yangilanadi. Misol: I_n - quyidagi giperparametrlarga ega bo‘lsin:

$$I_n=\{LR=0.01, BS=32, DR=0.2, LF="mse", NL=5, AF="relu"\}$$

Agar mutatsiyada tasodifiy tangangan giperparametr *LR* (o‘rganish tezligi) bo‘lib va yangi tasodifiy tanlangan qiymat 0.001 ga teng bo‘lsa, yangilangan $I_n^{'}$ individ quyidagicha bo‘ladi:

$$I_n^{'}=\{LR=0.001, BS=32, DR=0.2, LF="mse", NL=5, AF="relu"\}$$

Genetik algoritm *G=5* avlod davomida ishlaydi. Har avlodda *P=5* ta populyatsiya tanlanadi va keyingi avlodga genetik operatsiyalar qo‘llaniladi. Jarayon *P=0* dan boshlanib, avlodlarni rivojlantirish orqali eng yaxshi nazorat aniqligiga mos keluvchi giperparametrlar aniqlanib algoritm yakunalandi.

S-AESning 16-bitli shifrlash kalitlarini tasniflash uchun A1 algoritmiga asoslangan neyron tarmoq ADAM optimizatori bilan 10,000 davrda o‘qitildi. Sigmoid funksiyasi orqali qiymatlar 0 va 1 oralig‘iga keltirildi. Keras kutubxonasida Callback, ModelCheckpoint va EarlyStopping yordamida o‘quv jarayoni optimallashtirilib, 97,5% o‘quv aniqligi va 96,2% nazorat aniqligiga erishildi.

Dissertatsiyaning **“Nochiziqligi yuqori almashtirish komponentlarini shakllantirishning gibrid algoritmlari”** deb nomlangan uchinchi bobi statik va dinamik *S* komponentlarni shakllantirishga bag‘ishlanib, trigonometrik hamda Affin almashtirishlar bilan genetik algoritmni gibrid qo‘llash algoritmi ishlab chiqilgan.

3.1 paragrafda Genetik algoritm parametrlarida trigonometrik funksiyadan foydalanish orqali dinamik nochiziq almashtirish qiymatlarini shakllantirish algoritmi keltirilgan bo‘lib, trigonometrik funksiya sifatida quyidagi tanlangan:

$$f(z)=\sin((A+B)\cdot x\cdot z+C),$$

bu yerda, $0<x<1,\ 0\le z\le(2^n-1), B\in z$ va $A,C=\{1,3,...,2^n-1\}$.

Mazkur funksiyadagi *A, B, C* va *X* o‘zgaruvchilarini belgilangan qiymatlar oraliqlaridan tasodifiy tanlash orqali dinamik S-komponentlar generatsiya qilingan. Algoritmda *X*, *A* va *C* parametrlarini optimallashtirish orqali bardoshligi yuqori, **t**rigonometrik **f**unksiya **a**sosida shakllantirilgan (TFOSH) S_1 komponent berilgan.

3.2 paragrafda Affin almashtirishga genetik algoritmlarni qo‘llash orqali nochiziqligi yuqori statik komponentlarni shakllantirish algoritmi ishlab chiqilgan. Mazkur ishda $S\{8\times8\}$ komponentilarni hosil qilish AES shifrlash algoritmidagi usuldan foydalanilgan holda amalga oshirilgan. AES nochiziq almashtirish komponenti $GF(2^8)$ Galua maydonida keltirilmaydigan ko‘phad $m(x)=x^8+x^4+x^3+x+1$ orqali quyidagi funksiya bilan hisoblanadi.

$$S(x)=A\cdot x^{-1}+b,$$

bu yerda, A – 8×8 o‘lchamdagi binar matritsa va b – 8 o‘lchamdagi binar o‘zgarmas vektor. Tadqiqotda A matritsa chekli graf uchlari o‘rtasidagi munosabatni ifodalovchi qo‘shnilik matritsasi sifatida qaralgan. $n\times n$ o‘lchamdagi bu matritsa V va U to‘plamlaridan hosil qilinib, determinanti 0 ga teng bo‘lmagan xosmas matritsa sifatida belgilangan. Genetik algoritm yordamida xosmas qo‘shnilik matritsasini shakllantiruvchi **A2** algoritmi quyidagi qadamlardan iborat:

Kiruvchi parametrlar va ularning qiymatlari. n matritsa o‘lchami. m boshlang‘ich populyatsiya uchun generatsiya qilinish kerak bo‘lgan matritsalar soni. μ - mutatsiya ehtimoli, 0 dan 1 oraliqdagi haqiqiy son. Matritsa elementlarining o‘zgarish ehtimoli, φ-fitness funksiyada matritsaning determinantini aniqlash uchun kichik musbat haqiqiy son. t_{max} – maksimal avlodlar soni. p juftlar o‘rtasidagi krassover markazi, 0 dan n orasidagi butun son.

1-qadam. *Populyatsiyani tanlash*. m qo‘shni matritsadan iborat P_0 boshlang‘ich populyatsiya yaratiladi, bu yerda har bir A_i matritsa $n\times n$ o‘lchamli matritsadir. Matritsadagi har bir A_{ij} elementi 0 yoki 1 dan iborat.

2-qadam. *Fitness funksiya:* Fitness $f(A_i)$funksiya A_i qo‘shnilik matritsasining yaroqligini xos yoki xosmas matritsaga tekshirish orqali baholanadi.

$$f\left(A_i\right)=\begin{cases}\varphi, & agar\ \det\left(A_i\right)=0\\ \left|\det\left(A_i\right)\right|, & aks\,holda\end{cases},$$

bu yerda φ kichik musbat doimiy son.

3-qadam. A_i ning omon qolishi, ruletka g‘ildiragi usulidan foydalanilgan holda, fitness bahosi asosida aniqlanib ehtimoli uning yaroqliligiga mutanosibdir:

$$P_t\left(A_i\right)=f\left(A_i\right)\Big/\sum_{k=1}^{m}f\left(A_k\right)$$

4-qadam. Krassover uchun p tasodifiy nuqta tanlab olinib ikkita yangi A_{n1} va A_{n2} matritsalar asosiy (ota-ona) matritsalarning elementlarini aralashtirish orqali yaratiladi:

$$A_{n1}=\left[A_{p1}[1:p],\ A_{p2}[p+1:n]\right],\quad A_{n2}=\left[A_{p2}[1:p],\ A_{p1}[p+1:n]\right],$$

bu yerda A_{p1} va A_{p2} asosiy (ota-ona) matritsalari.

5-qadam. A_{ij} matritsaning har bir elementi μ ehtimol bilan mutatsiyalanadi.

$$A'_{ij}=\begin{cases}1-A_{ij}, & \mu\ ehtimollik\ bilan\\ A_{ij}, & aks\,holda\end{cases}$$

6-qadam. Yangi matritsa fitness funksiyasi bilan baholanadi. Agar xosmas matritsa topilmasa yoki avlodlar t_{max} ga yetgach algoritm yakunlanadi. Aks holda A'_{ij} yangi avlod matritsasini qayta shakllantirish uchun 2-qadamga o‘tiladi.

7-qadam. Xosmas qo‘shnilik matritsasi shartini qanoatlantirsa *nxn* matritsa qiymat sifatida olinib algoritm yakunlanadi.

Mazkur algoritmni Affin almashtirish generatsiyasiga qo‘llab statik S komponentlar shakllantirildi. Ularlarni nochiziqlik *N(f)*, umumiy nochiziqlik *N(S)*, algebraik immunitetlik *AI(S)*, qat’iy lavin samaradorlik *SAC*, Chiziqli yaqinlashish ehtimoli *LP*, differentsial bir xilligi *DU*, qo‘zg‘almas *FP* va qarama-qarshi qo‘zg‘almas *OFP* qiymatlar bo‘yicha baholash amalga oshirildi.

3.3 paragrafda genetik algoritm va affin almashtirish parametrlaridan gibrid usulda foydalanish orqali nochiziqligi yuqori dinamik *S*-komponentlarni shakllantiruvchi usul va algoritmlariga bag‘ishlanib, tajribaviy natijalar asosida quyidagi teoremalar aniqlandi:

1-teorema. Rinjdael algoritmida *m(x)* keltirilmaydigan ko‘phad bilan, *A* matritsa va Affin almashtirish $S(x) = A \cdot x^{-1} + b$ orqali hisoblangan S-komponenentning umumiy *N(S)* nochiziqligi 112 ni qanoatlantirsa *A* matritsani soat mili yoki teskasi bo‘yicha 90, 180, 270 gradusga burganda hosil qilingan *S*-komponentlarning umumiy nochiziqligi ham 112 ni qanoatlantiradi.

2-teorema. Affin almashtirishda *b* vektorning qiymati 0,0,0,0,0,0,0,0 yoki 1,1,1,1,1,1,1,1 ga teng bo‘lsa, $S(x) = A \cdot x^{-1} + b$ bilan hisoblangan nochiziq *S{8×8}* komponentning kamida 1 ta *FP* yoki qarama qarshi *OFP* nuqtasi mavjud bo‘ladi.

Affin almashtirishning keltirilgan va ko‘rib chiqilgan funksiyalar xossalari asosida quyidagi funksiya shakllantirildi.

$$S(x) = A_{2,r_2}^{d_2} \cdot \left(A_{1,r_1}^{d_1} \cdot x + b_1 \right)^{-1} + b_2$$

Shakllantirilgan Affin funksiyasi, *S(x)* chiqishini, *x* kirish qiymatini va A_1, A_2 lar *8×8* o‘lchamli binar matritsalarni o‘z ichiga oladi. Bularning har biri ma’lum bir d_1, d_2 qiymatlariga (1 yoki -1) va r_1, r_2 burilish burchaklariga (0, 90, 180, 270 daraja) ega. Shuningdek, har bir matritsa uchun b_1 va b_2 vektorlari mavjud. Bu parametrlar orqali 256 ta elementdan iborat dinamik *S(x)* komponentlarni shakllantiriladi, har bir *S(x)* nochiziqligi $N(S)_{min}$=112 ga teng. Buning uchun A_1 (1) va A_2 (2)matritsalari va *m(x)* o‘zgarmas, d_1, r_1 va d_2, r_2 esa o‘zgaruvchi parametrlar sifatida qaraldi. Jami kombinatsiyalar soni har bir d_1 va d_2 uchun 2 ta, har bir r_1 va r_2 uchun 4 ta, va b_1, b_2 uchun 254 tani tashkil etadi. Mazkur holat uchun $N(S)_{min}$=112ga teng bo‘lgan dinamik *S* nochiziqli komponentlarning jami kombinatsiyasi quyidagicha.

$$S_u = d_1 \times d_2 \times r_1 \times r_2 \times b_1 \times b_2 = 2 \times 2 \times 4 \times 4 \times 254 \times 254 = 4129024$$

S{8×8}-dinamik nochiziq almashtirish qiymatlarini hisoblash genetik algoritmdan foydalanib funksiyaning A_1 va A_2 parametrlari uchun (1) va (2) da ko‘rsatilgan matritsalar va keltirilmaydigan ko‘phad $m(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$ olindi.

$$A_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (1) \qquad A_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

Tanlangan qiymatlar **A**ffin **f**unksiya **o**rqali **sh**akllantirilgan (AFOSH) S_1 nochiziq komponenti shakllantirildi. Yuqorida tanlab olingan parametrlar bilan dinamik AFOSH komponentlarni shakllantirish uchun d_1, d_2, r_1 , r_2, b_1, *va* b_2 ning bazi

qiymatlari orqali AFOSH $S_2\{8\times8\}$, $S_3\{8\times8\}$, $S_4\{8\times8\}$, $S_5\{8\times8\}$ komponentlar hisoblandi.

Dissertatsiyaning **“Nochiziqli komponentlarni tasniflash va shakllantirish algoritmlari hamda dasturiy majmuasining natijalari tahlili”** deb nomlangan to‘rtinchi bobi nochiziq komponentlarni tasniflash va shakllantirish uchun takomillashtirilgan holda taklif etilgan algoritmlar, yaratilgan dasturiy majmua asosida nochiziq komponentlarni shakllantirish haqida bayon etadi. Ishlab chiqilgan ushbu algoritmlarning tajribaviy tadqiqotlar natijalari mavjud algoritmlar asosida olingan natijalar bilan qiyosiy tahlili va amaliy masalalar yechimlariga bag‘ishlanadi.

4.1-paragrafda giperparametrlarni optimallashtirish orqali kalitlarni tasniflash algoritmidan olingan natijalar tahlili shu turdagi boshqa tadqiqotlar bilan taqqoslandi. **M**ashinali **o‘**qitish **u**sullarini (MO‘U) S-AESning kalit bitlariga qo‘llash bo‘yicha tadqiqot natijalari tahlili 1-jadvalda berilgan. Bunda TNK-tasniflangan nochiziq komponent, TKU-tasniflangan komponent uzunligi, GPTU-giperparametrlarni tanlash usuli, O‘T-o‘quv tanlanma, NTA-nazorat tanlanma aniqligi, FTT-foydalanuvchi tomonidan tanlanganligi, GA-genetik algoritmni bildiradi. Olingan natijalar nazorat tanlanmada erishilgan eng yuqori tasniflash aniqligi bo‘yicha olindi. Tadqiqotda raund kalitlari uchun taklif etilgan usul SVM bilan amalga oshirilganda 13% gacha yuqori aniqligi, o‘quv tanlanma oldingi ishlardan 952 ta kam holatda amalga oshirilgan.

1-jadval.

MO‘Uni S-AES ning nochiziq komponentlarida qo‘llash natijalari

Tadqiqot ishi	MO‘U	TNK	TKU	GPTU	O‘T soni	NTA
H. Grari va boshq.(2022)	MLP	shifrlash kaliti	16	FTT	2400, 600	0.75
H. Kim va boshq.(2023)	RESNET		16	FTT	900000, 500000	0.69
Mazkur ish	MLP		48,16	GA	2048, 512	0.96
Mazkur ish	SVM	raund kaliti	32,48	Optuna	1024, 256	0.88

4.2-paragrafda statik va dinamik *S*-komponentlarini genetik algoritm orqali shakllantirish dasturiy majmuasi, tuzilishi va funksional imkoniyatlariga bag‘ishlangan. Dasturiy majmua, xosmas qo‘shnilik matritsalarini ajratish orqali yuqori nochiziqli *S*-komponentlarni shakllantirish bilan birga mavjud $S\{8\times8\}$ komponentlarning turli kriptografik talablarga bardoshliligini tekshirish imkoniyatini beradi.

4.3-paragrafda nochiziq almashtirishlarni shakllantirish algoritmlari natijalarining qiyosiy tahliliga bag‘ishlangan. Tadqiqotda ishlab chiqilgan algoritmlar orqali shakllantirilgan nochiziq *S*-komponentlarni boshqa tadqiqotlardagi komponentlar bilan bardoshlilik ko‘rsatkichlari taqqoslash amalga oshirildi. Ma’lumki 8 bitli kirish va chiqish qiymatlariga ega bo‘lgan balanslashgan nochiziq *S*-komponent uchun $N(S)=112$, $AI(S)=3$, $DU(S)=2$, $SAC(S)=0.5$, $FP(S)=0$, $OFP(S)=0$ va $AFP(S)=0$ qiymatlarga yaqin bo‘lishi muhim hisoblanadi.

2-jadvalda 3.2 paragrafda shakllantirilgan $S_1\{8\times8\}$, $S_2\{8\times8\}$ va $S_3\{8\times8\}$ komponentlar va boshqa tadqiqotchilar tomonidan taklif etilgan statik *S*-komponentlari minimal $N(f)_{min}$, maksimal $N(f)_{max}$ va umumiy $N(S)$ nochiziqligi, chiziqli kriptotahlilning korrelyatsiya matritsaning eng katta chetlanishi *LP*, differensial kriptotahlil uchun qurilgan ayirmalar matritsasining eng katta qiymati *DU*, qat'iy lavin samaradorlik *SAC*ning minimal, maksimal, o'rtacha, kvadratli og'ish qiymati, o'zgarmas va qarama qarshi o'zgarmas qiymatlari sonining yig'indisi *AFP* bo'yicha baholash natijalari berilgan.

2-jadval.

Statik *S*-nochiziq komponentlarni asosiy bardoshlilik me'zonlariga baholash

***S*-komponent**	**E'lon vaqti**	$N(f)_{max}$	$N(f)_{min}$	$N(S)$	$AI(S)$	LP	DU	$SAC(S)$				AFP
								min	**max**	**o'rta**	**kvad. og'ish**	
Mazkur ish S_1	2023	112	112	112	2	16	4	0.453	0.547	0.5	0.0276	0
Mazkur ish S_2	2023	112	112	112	2	16	4	0.453	0.531	0.5	0.0236	3
Mazkur ish S_3	**2024**	**112**	**112**	**112**	**2**	**16**	**4**	**0.453**	**0.531**	**0.5**	**0.0236**	**0**
N.Siddiqui v.b. S_7	2020	112	112	112	2	16	4	0.437	0.547	0.496	0.0286	2
Y.Wang v.b. S_1	2020	112	94	94	3	32	10	0.425	0.578	0.495	0.0324	3
Y.Wang v.b. S_1	2012	108	92	92	3	36	10	0.406	0.578	0.506	0.0380	5
Rinjdael AES	1998	112	112	112	2	16	4	0.453	0.562	0.504	0.0314	0
SM4, Xitoy	2016	112	112	112	2	16	4	0.437	0.562	0.499	0.0345	1
Kuznyechik	2015	116	100	100	3	28	8	0.437	0.609	0.512	0.0387	0
A. Razaq v.b. S_1	2022	112	96	96	3	34	10	0.453	0.562	0.501	0.0261	4
A. Razaq v.b. S_1	2023	112	108	108	2	20	6	0.421	0.578	0.501	0.0364	3
M. Ahmad v.b. S_1	2016	110	92	92	3	36	10	0.406	0.594	0.498	0.0418	1

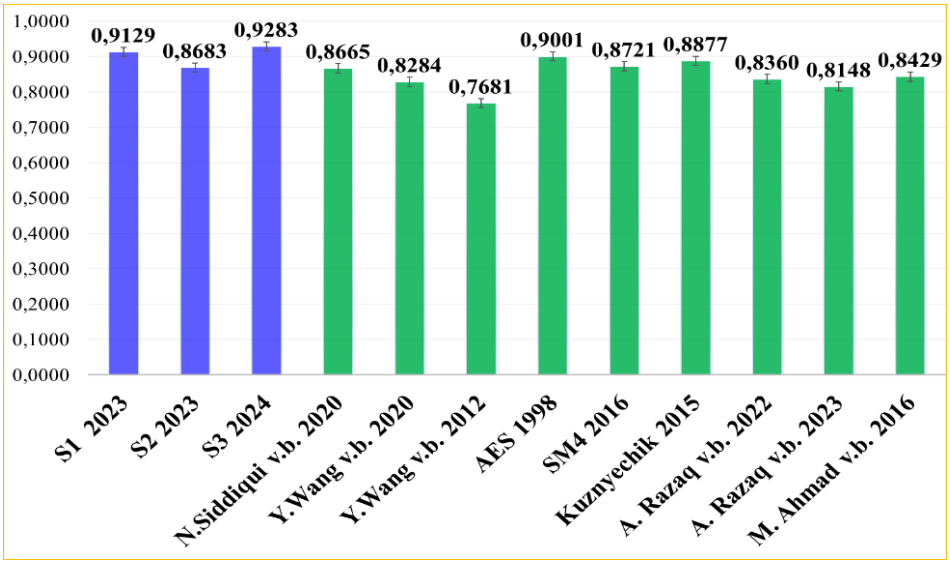
Ko'rib chiqilgan bardoshlilik mezonlari va ularning tavsiyaviy qiymatlari asosida S{8×8} komponentlar uchun **u**mumuiy **b**ardoshlililik **k**o'rsatgich *UBK*ni (3) hisoblash amalga oshirildi. Bunda $SAC_{o'rt}$ ni hisoblashda (4), *AFP* uchun (5) o'rinli.

$$UBK = \left(\begin{array}{l} \frac{N(f)_{\min}}{112} + \frac{N(f)_{\max}}{120} + \frac{N(S)}{112} + \frac{AI(S)}{3} + \frac{258 - DU}{256} + \\ + \frac{SAC_{\min}}{0.5} + \frac{1 - SAC_{\max}}{0.5} + \frac{SAC_{o'rt}}{0.5} + \frac{0.02}{SAC_{kv\,xato}} + AFP \end{array} \right) / 10 \quad (3)$$

$$SAC_{o'rt} = \begin{cases} \frac{0.5}{SAC_{o'rt}}, agar\ SAC_{o'rt} > 0.5\ bo'lsa, \\ 1,\ agar\ SAC_{o'rt} = 0.5\ bo'lsa. \\ \frac{1 - SAC_{o'rt}}{0.5}, aks\ holda. \end{cases} \quad (4)$$

$$AFP = \begin{cases} 1 - AFP / 5,\ agar\ 5 >= AFP\ bo'lsa, \\ 0,\ aks\ holda. \end{cases} \quad (5)$$

Ushbu (5) ifoda orqali S-komponent qiymatlari hisoblansa *UBK* ning maksimal ko‘rsatgichi *UBK=1* bo‘ladi. 2-jadvalda berilgan talablarga baholash qiymatlarini (5) formulaga qo‘yish orqali *UBK* hisoblanib uning natijalari va vizual grafigi 2-rasmda berilgan.



2-rasm. Statik *S*-komponentlarning UBK ko‘rsatgichlari

Affin almashtirish va genetik algoritm asosida shakllangan dinamik S-komponentlarining ba’zi parametrlar bilan hisoblangan qiymatlari va bardoshlilik tahlili 3-jadvalda berilib, boshqa ishlar bilan taqqoslandi.

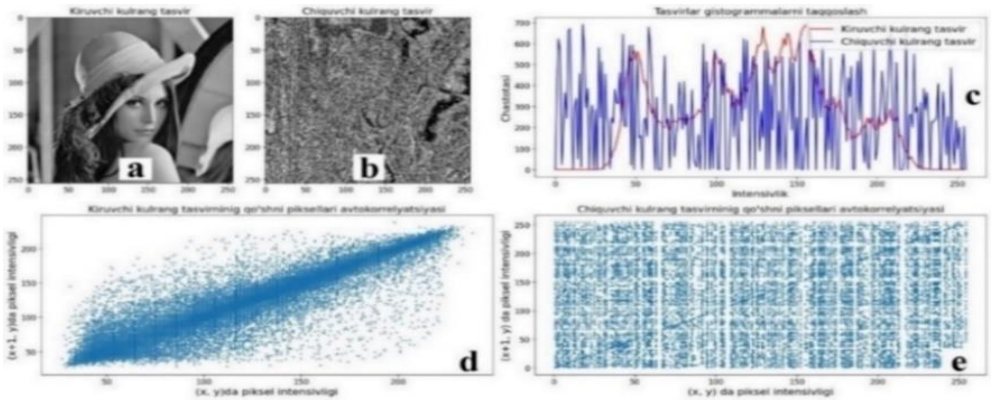
3-jadval.

Dinamik *S*-komponentlarni kriptografik me’zonlariga baholash

***S*-komponent**	***E'lon vaqti***	***N(f)max***	***N(f)min***	***N(S)***	***AI(S)***	***LP***	***DU***	***SAC(S)***				***AFP***
								min	***max***	***o‘rta***	***kv. og‘ish***	
TFOSH S_1	2023	112	94	94	3	34	10	0.391	0.578	0.494	0.044	1
AFOSH S_1	**2024**	**112**	**112**	**112**	**2**	**16**	**4**	**0.453**	**0.547**	**0.5**	**0.027**	**0**
AFOSH S_2	2024	112	112	112	2	16	4	0.437	0.562	0.499	0.030	0
C.B.Erendira v.b.	2023	110	96	96	2	32	12	0.391	0.594	0.501	0.043	1
O‘zDSt.1105:2009	2014	108	92	92	3	36	10	0.375	0.625	0.496	0.046	0
A.H.Zahid v.b.	2021	112	96	96	3	32	10	0.437	0.562	0.506	0.033	1
K.Abdullah v.b.	2021	112	96	96	3	32	12	0.391	0.578	0.496	0.039	5
A.H.Zahid v.b.	2020	110	92	93	3	36	10	0.406	0.594	0.498	0.042	2
S.Hussain v.b.	2020	110	96	96	3	28	12	0.422	0.631	0.511	0.038	1

S-komponentini tasvirlar asosida statistik tahlil qilish me’zonlaridan entropiya *H*, kontrast *K*, korrelyatsiya ρ, gomogenlik *G*, energiya *E* va **A**bsolyut **o**g‘ishning o‘rtacha **q**iymati (*AOQ*) kabi parametrlarga baholandi. Ushbu me’zonlar tasvir piksellarining *S*-komponentga kiruvchi va chiquvchi qiymatlar o‘rtasidagi diffuziya va tasodifiylik darajasini o‘lchab uning umumiy samaradorligini aniqlaydi. Baholash uchun boshqa ishlarda qo‘llanilgan *256×256* o‘lchamli Lena, maymun va bolgar qalampiri, tasvirlari tanlandi.

Har bir tasvir dastlab kulrang tasvir holatiga o‘tkazilib, *S*-komponentga kiritilgan holda, chiquvchi qiymatlardan *256×256* o‘lchamli tasvir hosil qilindi hamda yuqorida keltirilgan mantiqiy mezonlar asosida baholandi. Lena tasviri uchun hisoblangan natijalar 4-jadvalda, uning natijalari asosida S_3 statik komponentga Lena tasviri kiritib undan chiquvchi tasvir, gistogrammasi va qo‘shni piksellari avtokorrelyatsiyasi grafiklari 3-rasmda berildi.



3-rasm. Lena (a) tasvirini S_3 ga kiritilishdan hosil bo‘lgan tasvir (b), ularning gistogramma (c) hamda qo‘shni piksellari avtokorrelyatsiyasi (d), (e).

4-jadval.

Lena tasvirida S-komponentlarni mantiqiy mezonlarga baholash natijalari

S-komponent	*H*	*K*	*ρ*	*E*	*G*	*AOQ*
Lena tasviri	7.423	256.21	0.9428	0.0183	0.2193	-
Mazkur ish, statik S_3	7.423	9563.15	0.0994	0.0183	0.0988	**135.85**
Dinamik AFOSH S_1	7.423	10768.38	0.0760	0.0183	0.0972	124.21
AES, AQSH	7.423	10968.52	0.0751	0.0183	0.0968	116.25
SM4, Xitoy	7.423	9572.14	0.1194	0.0183	0.0976	131.95
Kuznyechik, Rossiya	7.423	9647.07	0.1020	0.0183	0.0990	130.85
O‘zDSt 1105:2009	7.423	9850.39	0.0520	0.0183	0.0966	132.80
Y.Wang va boshq. S_1	7.423	9533.94	0.0923	0.0183	0.0969	130.36

Olingan natijalarni solishtirish (2-4 jadvallarga qarang) taklif qilingan usul va algoritmlar S-AES kalitlarini tasniflash aniqligi bo‘yicha boshqalardan o‘rtacha 13%ga, shakllantirilgan statik S-komponent *UBK* bo‘yicha boshqalardan o‘rtacha 8,2% ga yuqori bardoshli xususiyatiga erishdi. Dinamik nochiziq *S*-komponentlar *UBK* bo‘yicha boshqalardan o‘rtacha 6,8% ga yuqori natija ko‘rsatdi. Tasvirlarga asoslangan statistik me’zonlarda Lena tasvirida statik S_3 komponent *AOQ* bo‘yicha boshqa komponentlardan 3,05 dan 19,6 gacha yuqori natija ko‘rsatdi. Olib borilgan tadqiqot natijalari va hisoblash eksperimentlari taklif etilgan algoritmlarning afzalligini ko‘rsatdi.

Dissertatsiyaga ilovalarda tadqiqot natijalarining amaliy qo‘llanilishini tasdiqlovchi hujjatlarning nusxalari hamda O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk Agentligi tomonidan berilgan dasturlarni rasmiy ro‘yxatga olinganligi to‘g‘risidagi guvohnomalarning nusxalari keltirilgan.

XULOSA

“Nochiziqli komponentlarni shakllantirish va tasniflash algoritmlari” mavzusida olib borilgan dissertatsiya tadqiqotining asosiy natijalari quyidagilardan iborat:

1. Nochiziqligi yuqori bo‘lishi talab etiluvchi algoritmlar sifatida simmetrik shifrlash algoritmlarining nochiziq komponentlari sifatida kalit bitlari va nochiziq *S* komponent tanlanib, tasniflash hamda shakllantirish muammolari tahlil qilindi. Tahlil natijasida mashinali o‘qitish usullari hamda genetik algoritmlarni simmetrik kalitli blokli shifrlarning nochiziqli komponentlariga qo‘llash usullari va algoritmlari aniqlandi.
2. Soddalashtirilgan S-AES simmetrik kalitli shifrlash algoritmninig asosiy va raund kalit bitlarini tasniflash uchun tanlangan ochiq matn, *S* komponent va shifrlangan matn asosida o‘quv va nazorat tanlanmalarni shakllantirish yondashuvi taklif etildi. Mazkur yondashuv S-AES algoritmining kalit bitlarini samarali tasniflash imkonini beradi.
3. S-AES kalit bitlarini tasniflashda Optuna dasturi yordamida SVM giperparametrlari tanlandi, SNT arxitekturasini qurish uchun genetik algoritm ishlab chiqildi. Ushbu algoritmlar modelning umumlashtirish qobiliyatini yaxshilab, kalit bitlarini tasniflashda oldingi tadqiqotlarga nisbatan 952 ta kam o‘quv tanlanmada, nazorat aniqligi 13% ga oshirish imkonini berdi.
4. Genetik algoritm yordamida *A* xosmas matritsani tanlab uni affin almashtirishda qo‘llash orqali statik nochiziq S_3 komponent shakllantirildi. S_3 komponent 1998-2023 yillarda o‘tkazilgan tadqiqotlar bilan taqqoslagan umumiy bardoshlilik ko‘rsatgichi bo‘yicha AQSHning AES standartidan 2,8%ga, Rossiya Federatsiyasi Kuznyechik algoritmidan 4%ga, Xitoyning SM4 shifrlash standartlaridan 5,6%ga yuqori bardoshligiga erishish imkonini berdi.
5. Tadqiqotda genetik algoritm parametrlarida kriptografik baholashni inobatga olgan holda dinamik nochiziq *S* komponentlarni shakllantirish algoritmi taklif etildi. Mazkur algoritm bardoshliligi yuqori dinamik *S* komponentlarni shakllantirish imkonini berdi. Tadqiqot natijalari O‘zDSt 1105:2009 shifrlash standartida qo‘llanilayotgan dinamik *S* komponentiga nisbatan umumiy nochiziqligi *N(S)* 16-20 ga umumiy bardoshlilik ko‘rsatgichi 7%ga, shuningdek, boshqa *S* komponentlari bilan solishtirganda umumiy bardoshlilik ko‘rsatgichi bo‘yicha 6,8% ga yaxshilanishiga erishildi.
6. Tadqiqotda taklif etilgan giperparametrlarni optimallashtirish algoritmi neyron tarmoqning ko‘p qatlamli perseptron usuli yordamida tasniflanadigan masalalarni yechish imkonini beradi.
7. Statik va dinamik *S* komponentlarni shakllantirish algoritmi asosida ishlab chiqilgan dasturiy ta’minotni simmetrik kalitli shifrlash algoritmlari standartlarini loyihalashda foydalanish mumkin. Bu mazkur algoritmlarining turli kriptotahlil usullariga bardoshliligi oshirish imkonini beradi.

НАУЧНЫЙ СОВЕТ DSc.03/26.05.2022.T.10.05 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ НАЦИОНАЛЬНОМ ИССЛЕДОВАТЕЛЬСКОМ УНИВЕРСИТЕТЕ «ТАШКЕНТСКИЙ ИНСТИТУТ ИНЖЕНЕРОВ ИРРИГАЦИИ И МЕХАНИЗАЦИИ СЕЛЬСКОГО ХОЗЯЙСТВА»

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

АБДУРАЗЗОКОВ ЖАВОХИР РУСТАМОВИЧ

АЛГОРИТМЫ ФОРМИРОВАНИЯ И КЛАССИФИКАЦИИ НЕЛИНЕЙНЫХ КОМПОНЕНТОВ

05.01.03 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации доктора философии (PhD) по техническим наукам

Ташкент – 2024

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована за номером B2024.1.PhD/T4410 в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан.

Диссертация выполнена в НИИ развития цифровых технологий и искусственного интеллекта.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице Научного совета (www.tiiame.uz) и на информационном образовательном портале "Ziyonet" (www.ziyonet.uz).

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
Официальные оппоненты:	**Мирзаев Номаз** доктор технических наук, профессор
	Ходиев Шухрат Илхамович кандидат технических наук, доцент
Ведущая организация:	**Самаркандский государственный университет имени Шарофа Рашидова**

Защита диссертации состоится «22» ноября 2024 года в 14⁰⁰ часов на заседании Научного совета DSc.03/26.05.2022.T.10.05 при Национальном исследовательском университете «Ташкентского института инженеров ирригации и механизации сельского хозяйства» (Адрес: 100000, г. Ташкент, ул. Кари Ниязи, 39. Тел: (99871) 237-19-36; факс: (99871) 237-54-79; e-mail: admin@tiiame.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре при Национальном исследовательском университете «Ташкентского института инженеров ирригации и механизации сельского хозяйства» (зарегистрировано №342). (Адрес: 100000, г. Ташкент, ул. Кари Ниязи, 39. Тел.: (99871) 237-19-45).

Автореферат диссертации разослан «12» 11 2024 года.

(реестр протокола рассылки №7 от «11» 11 2024 года)

Н.С.Маматов
Председатель Научного совета
по присуждению ученых степеней,
доктор технических наук, профессор

Д.К.Бекмуратов
Ученый секретарь Научного совета
по присуждению учёных степеней,
доктор философии по техническим наукам (PhD)

С.С.Раджабов
Председатель Научного семинара
при Научном совете по присуждению
ученых степеней, доктор технических наук,
старший научный сотрудник

Введение (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В мире, с развитием информационных технологий и увеличением объёмов цифровых данных, вопрос обеспечения их безопасности становится всё более сложным. В условиях, когда объём данных настолько велик, что ручная обработка невозможна, всё большую роль играют методы машинного обучения. Блочные симметричные алгоритмы шифрования с секретным ключом являются защиты информации, так как они эффективны и надёжны в противодействии киберугрозам. Однако современные кибератаки требуют постоянного совершенствования таких алгоритмов и внедрения новых технологий. Одним из перспективных направлений является использование машинного обучения и эволюционных алгоритмов для повышения эффективности шифрования. Это направление активно исследуется учёными из таких стран, как США, Индия, Китай, Россия, Германия и Япония, которые разрабатывают теоретические и практические подходы к улучшению блочных шифров.

В мире, с развитием угроз в области кибербезопасности, возникает необходимость повышения эффективности алгоритмов симметричного шифрования. Важные исследования сосредоточены на применении искусственного интеллекта и генетических алгоритмов для оптимизации процессов шифрования, создания нелинейных компонентов и повышения устойчивости к атакам. Одной из основных задач является выбор функций для формирования высоконелинейных компонентов, что позволяет усилить алгоритмы против современных угроз. Также важна правильная классификация битов ключей и настройка гиперпараметров в методах машинного обучения. Применение эволюционных алгоритмов помогает улучшить безопасность, управляя ключами и анализируя уязвимости, что в совокупности делает алгоритмы шифрования более надёжными. Учёные из разных стран активно разрабатывают методы для оценки надёжности и совершенствования современных систем шифрования.

В Республике Узбекистан внедрение информационно-коммуникационных технологий во все экономические и социальные сферы является одним из основных направлений современного прогресса. В Стратегии «Цифровой Узбекистан – 2030»[3] предусмотрены задачи по изучению и внедрению в практику возможностей искусственного интеллекта, криптографии и машинного обучения в отраслях экономики, обеспечению информационной безопасности инфраструктур и защиты документов, а также защите информации для государственных органов, физических и юридических лиц., «О дополнительных мерах по развитию образования и науки в области криптологии в Республике Узбекистан» обозначены задачи по увеличению масштабов научных исследований в данной области и их практической значимости, а также по созданию современных методов

[3] Указ Президента Республики Узбекистан от 5 октября 2020 года УП-6079 «Об утверждении стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации»

криптоанализа[4]. Выполнение данных задач включает в себя усовершенствование симметричных шифровальных алгоритмов, которые играют важную роль в информационной защите, с помощью машинного обучения и генетических алгоритмов, а также их оценку через современные криптоанализы, что является одной из важнейших задач. Постановлением Президента Республики Узбекистан №ПП-4699 «О мерах по широкому внедрению цифровой экономики и электронного правительства» от 28 апреля 2020 года, №ПП-4996 «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» от 17 февраля 2021 года, а также другими нормативно-правовыми документами, принятыми в данной сфере в определенной степени служит настоящее диссертационное исследование.

Соответствие исследования приоритетным направлениям развития науки и технологий Республики. Данное исследование выполнено в рамках приоритетного направления развития науки и технологий Республики IV «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Научные исследования по вопросам классификации и формирования нелинейных компонентов симметричных алгоритмов шифрования с использованием методов машинного обучения и генетических алгоритмов были проведены такими учёными, как N.Kopal, R.Rivest, L.Lerman, A.Benamira, M.Perusheska, Y.Alsariera, A.Petrov, H.Kim, X.Yin, W.Zhang, A.Zahid, A.Kokcham, S.Omran, Y.Wang и рядом др.

Также вопросы применения методов машинного обучения и генетических алгоритмов для классификации нелинейных данных и поиска оптимальных решений в различных задачах нашли отражение в научных работах узбекских учёных Т.Ф.Бекмуратова, М.М.Камилова, Ш.Х.Фазилова, Ф.Т.Адиловой, Д.Т.Мухаммедиевой, Р.Х.Хамдамова, Н.А.Игнатьева, Н.С.Маматова, Х.А.Примовой, С.С.Раджабова и других учёных. Вопросы разработки шифровальных алгоритмов, формирования их криптографических нелинейных компонентов и оценки их стойкости были предметом исследований научных коллективов под руководством М. Арипова, П.Ф. Хасанова, С.К. Ганиева, Б.Ф. Абдурахимова, М.М. Каримова, Д.Ю. Акбарова, Г.У. Жураева, Г.Н. Туйчиева, Д.М. Курязова, А.Б. Саттарова и других учёных.

Кроме того, вопросам применения методов машинного обучения и генетических алгоритмов для классификации и формирования нелинейных компонентов симметричных алгоритмов шифрования не было уделено достаточного внимания.

Связь диссертационного исследования с планами научно-исследовательских работ научно-исследовательского учреждения, в котором была выполнена диссертация. Диссертационное исследование выполнено в рамках проекта фундаментальных исследований под номером

[4] Постановление Президента Республики Узбекистан от 15 августа 2024 года ПП-293 «О дополнительных мерах по развитию образования и науки в сфере криптологии в Республике Узбекистан»

ФЗ-20200929308 «Создание теоретических основ интегрированных технологий биометрической авторизации пользователей в системах обеспечения информационной безопасности» (2021–2023) согласно плану научно-исследовательских работ НИИ развития цифровых технологий и искусственного интеллекта.

Цель исследования. Разработка алгоритмов классификации и формирования высоконелинейных компонентов симметричных блочных шифров с использованием методов машинного обучения и генетических алгоритмов.

Задачи исследования:

анализ современных подходов к применению методов машинного обучения и генетических алгоритмов к нелинейным компонентам шифровальных алгоритмов;

разработка подхода к формированию обучающих и контрольных выборок на основе нелинейных компонентов симметричных шифровальных алгоритмов;

формирование подхода к повышению точности классификации раундовых ключей на основе оптимизации гиперпараметров метода опорных векторов;

разработка алгоритма классификации битов шифровального ключа на основе применения генетического алгоритма в архитектуре нейронных сетей;

разработка алгоритма формирования значений статических нелинейных компонентов на основе разложения матрицы смежности с помощью генетического алгоритма и его применения в аффинной функции;

разработка алгоритма формирования значений динамических нелинейных компонентов с учётом криптографической оценки в параметрах генетического алгоритма;

разработка программного комплекса для формирования нелинейных компонентов и проведение вычислительных экспериментов.

Объектом исследования являются процессы классификации и формирования нелинейных компонентов симметричных блочных шифровальных алгоритмов.

Предметом исследования являются применение методов машинного обучения для классификации ключей симметричных шифровальных алгоритмов, а также разработка алгоритмов и программного обеспечения для формирования статических и динамических значений нелинейного компонента подстановки (S-блок), обеспечивающего высокую стойкость.

Методы исследований. Теоретические исследования работы выполнены на основе методов математического анализа, дискретной математики, теории вероятностей и математической статистики, вычислительной математики, прикладной криптографии и криптоанализа.

Научная новизна исследования заключается в следующем:

на основе нелинейных компонентов симметричных шифровальных алгоритмов предложен подход к формированию обучающих и контрольных выборок;

на основе оптимизации гиперпараметров метода опорных векторов предложен подход к повышению точности классификации раундовых ключей;

на основе применения генетического алгоритма в архитектуре нейронной сети разработан алгоритм классификации битов шифровального ключа;

разработан алгоритм формирования значений статических нелинейных компонентов на основе разложения матрицы смежности с помощью генетического алгоритма и его применения в аффинной функции;

разработан алгоритм формирования значений динамических нелинейных компонентов с учётом криптографической оценки в параметрах генетического алгоритма.

Практические результаты исследования заключаются в следующем**:**

разработан алгоритм выбора гиперпараметров методов машинного обучения для повышения точности классификации нелинейных данных;

алгоритм выбора гиперпараметра алгоритм блочного шифрования с симметричным ключом применялся при классификации битов ключа;

разработан алгоритм формирования статического нелинейного компонента подстановки с 256 значениями, обладающего высокой стойкостью;

разработан алгоритм и программный комплекс для формирования значений динамических нелинейных компонентов с учётом криптографической оценки в параметрах генетического алгоритма.

Достоверность результатов исследования. Надёжность результатов исследования объясняется корректной постановкой задачи в отношении нелинейных компонентов симметричных шифровальных алгоритмов, а также сравнительным анализом разработанных алгоритмов с реальными и экспериментальными результатами.

Научно-практическая значимость результатов исследования.

Научная значимость полученных в исследовании результатов заключается в том, что точность классификации битов ключа симметричного блочного шифровального алгоритма была улучшена за счёт выбора гиперпараметров метода опорных векторов и нейронной сети с применением современных методов оптимизации и генетического алгоритма, а также в том, что алгоритмы формирования нелинейных S компонентов обеспечили высокую стойкость к криптографическим атакам.

Практическая значимость результатов исследования объясняется возможностью применения разработанных алгоритмов и программного обеспечения для решения задач классификации нелинейных данных, а также в раундовых функциях современных симметричных блочных шифров.

Внедрение результатов исследования. На основе разработанных в исследовании алгоритмов формирования и классификации нелинейных компонентов, а также программного комплекса:

алгоритм классификации, разработанный на основе нейронной сети с оптимизацией гиперпараметров с использованием генетического алгоритма, был внедрён в Центре цифровизации и хранения данных управления статистики Сурхандарьинской области (справка Хокимията Сурхандарьинской области от 23 сентября 2024 года № 07-07/1988). В

результате разработанный алгоритм позволил улучшить прогнозирование данных об экономических показателях на 8-10% и сократить время обработки на 11-13%.

в исследовании программный комплекс, созданный путем замены внутреннего нелинейного блока подстановки AES на S-компонент, сформированный на основе генетического алгоритма, был внедрен в Сурхандарьинском областном территориальном отделении Министерства цифровых технологий с целью шифрования больших объемов данных (справка Хокимията Сурхандарьинской области от 23 сентября 2024 года № 07-07/1988). В результате, при вводе ста тысяч случайных открытых текстов и ключей, по сравнению с существующим алгоритмом AES, удалось сократить время шифрования на 11,5-12,5% и разшифровки на 10,5-12%;

в исследовательской работе сформированный статический *S* компонент был внедрён в процесс обмена информацией в ООО "Центр развития информационно-коммуникационных технологий" при Сурхандарьинская управления по управлению государственными активами с целью обеспечения безопасности беспроводной локальной сети и оценки эффективности процесса шифрования данных (справка Хокимията Сурхандарьинской области от 23 сентября 2024 года № 07-07/1988). В результате статический S-компонент позволил достичь среднего показателя устойчивости на 12,5% выше, чем внутренний нелинейный блок подстановки стандарта шифрования AES;

в исследовании программный комплекс, разработанный на основе сформированного S-компонента, был внедрён в филиале IT-парка Термеза Сурхандарьинской области с целью защиты больших объёмов данных (справка Хокимията Сурхандарьинской области от 23 сентября 2024 года № 07-07/1988). В результате, ввод случайного одного миллиона открытых текстов и ключей в комплекс позволил сократить времени на 13-15% при сравнении с алгоритмом AES для полученных шифротекстов.

в ходе исследования статический компонент S, сформированный на основе генетического алгоритма, был внедрён вместо компонента S в китайском алгоритме шифрования SM4, что было реализовано в компании Inner Mongolia Wangxin Information Security Service Co., Ltd. (справка № WXSEC20240410005 от 10 апреля 2024 года, предоставленная Inner Mongolia Wangxin Information Security Service Co. Ltd). В результате стойкость алгоритма шифрования SM4 удалось улучшить на 13-13,5% в среднем.

Апробация результатов исследования. Основные положения и результаты диссертационной работы докладывались и обсуждались на 4 международных и 5 республиканских конференциях.

Публикация результатов исследования. По теме диссертации опубликовано 21 научных работ, в том числе 9 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, из них 4 в республиканских и 5 в зарубежных журналах (4 статьи индексированные в Scopus), получены 3 свидетельства об официальной регистрации программы для ЭВМ.

Структура и объем диссертации. Диссертация содержит 120 страниц и состоит из введения, четырех глав, заключения, списка использованной литературы и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность и необходимость темы диссертации, показано соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, определены цели и задачи, а также уточнены объект и предмет исследования. Обоснована достоверность полученных результатов, приведена информация о их теоретической и практической значимости, внедрении результатов исследования на практике, опубликованных работах и структуре диссертации.

В первой главе диссертации под названием «Анализ проблем формирования и классификации компонентов алгоритмов с высокой нелинейностью» проведён анализ методов и алгоритмов интеллектуального анализа данных, а также современного состояния симметричных блочных шифровальных алгоритмов. Задача классификации рассмотрена с учётом шифрования и раундовых ключей симметричного алгоритма, выявлены проблемы их классификации. Изучены вопросы формирования нелинейных S-компонентов в блочных шифровальных алгоритмах, описаны новые результаты и алгоритмы, разработанные с помощью генетического алгоритма.

В параграфе 1.1 рассмотрены методы интеллектуального анализа данных, включая метод опорных векторов (SVM) и искусственные нейронные сети (ИНС). Исследованы проблемы выбора гиперпараметров, которые существенно влияют на качество решений. Отмечено, что эти методы эффективны для задач бинарной классификации, однако выбор гиперпараметров имеет ключевое значение.

В параграфе 1.2 представлены данные об алгоритмах, компоненты которых должны обладать нелинейностью, и их анализ. Рассмотрены современные блочные шифры, их роль в защите данных, внутренняя структура и обзор нелинейных компонентов этих алгоритмов.

В параграфе 1.3 проанализированы критерии оценки нелинейных S-компонентов. Основными параметрами для их криптографической безопасности указаны: нелинейность, вероятность дифференциального приближения, строгое лавинное свойство, алгебраический иммунитет, фиксированные и противоположные фиксированные точки. Подчёркнута важность оценки этих критериев и предложены их рекомендуемые значения.

В параграфе 1.4 проанализированы проблемы формирования и классификации нелинейных компонентов, а также применение машинного обучения в симметричных блочных шифрах для повышения их безопасности. Отмечено, что создание стойкого S-компонента сложная задача. Использование генетических алгоритмов для формирования S-компонентов представляет новый подход, позволяющий оптимизировать ключевые криптографические параметры, такие как нелинейность.

В параграфе 1.5 была поставлена следующая исследовательская задача: в качестве нелинейных компонентов были выбраны биты ключей симметричных блочных шифров и нелинейный компонент подстановки S, при этом задачи исследования были сформулированы следующим образом. Для задачи классификации дан набор открытых текстов $\mathcal{P} = \{P_1, P_2, \ldots, P_i\}$, где каждый элемент обозначен как $P_i \in \{0,1\}^m$. Набор битов ключа обозначен как $\mathcal{K} = \{K_1, K_2, \ldots, K_i\}$, где каждый элемент $K_i \in \{0,1\}^n$. Набор шифротекстов обозначен как $\mathcal{C} = \{C_1, C_2, \ldots, C_i\}$, где каждый элемент $C_i \in \{0,1\}^m$. Длина битов открытого и зашифрованного текста обозначена как *m*, а длина ключа как *n*. Функция шифрования $E : \mathcal{K} \times \mathcal{P} \to \mathcal{C}$ задается как $E(K_i, P_i) = C_i$, где K_i это ключ, а P_i-открытый текст, что в результате приводит к шифротексту C_i. Необходимо разработать модель машинного обучения для классификации ключа K_i, использованного при шифровании, на основе данных пар (P_i, C_i). Формируемый S-компонент является ключевым элементом симметричных шифров и должен обладать высокой нелинейностью, строгим лавинным свойством, низкой вероятностью дифференциального приближения, а также отсутствием неподвижных и противоположных точек. Это подчёркивает важность создания S-компонентов, соответствующих этим критериям.

Вторая глава диссертации под названием **«Алгоритмы классификации высоконелинейных компонентов»** посвящена методам классификации раундов и битов шифровального ключа в упрощённых симметричных алгоритмах, подготовке сформированных нелинейных данных для обучения, а также разработке алгоритмов выбора гиперпараметров для SVM и ИНС.

В параграфе 2.1 рассмотрены классические шифры, такие как аффинный, Виженера и Плейфера, для получения шифротекстов как нелинейных данных. Для их классификации применена ИНС, показавшая точность обучения свыше 95% и тестирования более 79%. Это демонстрирует потенциал методов машинного обучения в криптоанализе и их возможное применение для анализа современных блочных шифров.

В параграфе 2.2 использовался упрощённый S-AES для классификации битов шифровального ключа. Входными данными были пары открытого и зашифрованного текста, а выходными — биты ключа. Эксперименты с ИНС показали проблему оптимального выбора гиперпараметров при классификации ключей S-AES.

В параграфе 2.3 для классификации битов ключа S-AES раунды шифрования и распределение ключей были разделены на две части. В первой использовались биты ключа *k* и раундовые ключи *KP, KF, KS* для обучения. Во второй - случайный ключ *k* и его раундовые ключи. Сгенерированы шифротексты c_1 и c_2 для открытых текстов p_1=1000100010001000 и p_2=1100110011001100, использован нелинейный компонент S_b*={9,4,A,B,D,1,8, 5,6,2,0,3,C,E,F,7}*. Эти данные сформировали обучающую выборку для SVM, где каждый бит раундового ключа классифицировался отдельно.

Оптимальные гиперпараметры были выбраны с помощью программы Optuna через 1000 испытаний.

Гиперпараметры SVM, θ - и их область поиска включали $C=[10^{-3}, 10^{3}]$ а также различные ядровые функции: линейные, полиномиальные, радиально-базисные и сигмоидальные, для которых параметры подбирались в заданных числовых интервалах.

$$S_K = \begin{bmatrix} kp_{1,1} & kp_{1,2} & \cdots & kp_{1,n} & kf_{1,1} & kf_{1,2} & \cdots & kf_{1,n} & ks_{1,1} & ks_{1,2} & \cdots & ks_{1,n} & k_{1,1} & k_{1,2} & \cdots & k_{1,n} \\ kp_{2,1} & kp_{2,2} & \cdots & kp_{2,n} & kf_{2,1} & kf_{2,2} & \cdots & kf_{2,n} & ks_{2,1} & ks_{2,2} & \cdots & ks_{2,n} & k_{2,1} & k_{2,2} & \cdots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ kp_{N,1} & kp_{N,2} & \cdots & kp_{N,n} & kf_{N,1} & kf_{N,2} & \cdots & kf_{N,n} & ks_{N,1} & ks_{N,2} & \cdots & ks_{N,n} & k_{N,1} & k_{N,2} & \cdots & k_{N,n} \end{bmatrix}$$

В результате эксперимента максимальная точность классификации составила 88,46%, минимальная – 61,54%, а средняя – 70,67%.

Для формирования обучающих выборок для битов шифровального ключа было выбрано $N=2048$ случайных 16-битных ключей k. Эти ключи вводились в часть распределения ключей S-AES, где генерировались раундовые субключи *(KP, KF, KS)*, образующие набор из 48 бит.

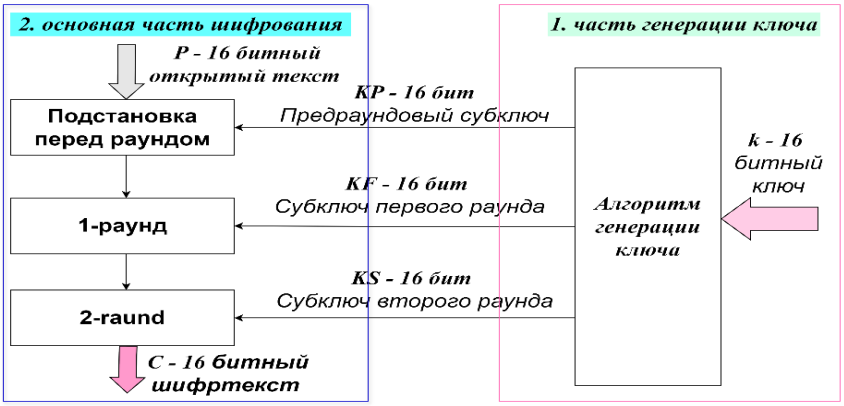


Рис. 1. Части S-AES при формировании обучающих выборок

Для классификации ключа k по раундовым ключам была сформирована обучающая выборка в виде S_K. Сформированная обучающая выборка для ИНС включает входные данные x_n, представляющие субключи kp, kf и ks, сгенерированные на основе случайного ключа k. Для выхода y_n были созданы отдельные выборки для классификации каждого бита ключа k. Генетический алгоритм **A1** для подбора гиперпараметров и построения архитектуры ИНС включает следующие шаги:

Входные параметры и их значения: обучающая выборка, гиперпараметры ИНС и их числовые диапазоны.

Выходной результат: гиперпараметры, обеспечивающие наивысшую точность классификации на контрольной выборке для данного выходного класса, который требуется классифицировать на основе обучающей выборки.

Шаг 1. Обозначим все возможные наборы гиперпараметров как H. Каждый гиперпараметр $h_i \in H$ принимает значения из заранее определённого диапазона. Для данной задачи были установлены следующие параметры: Функции активации $AF \in \{"relu","elu","selu","prelu","gelu"\}$, процент отсева

$DR \in \{0.1, 0.2, 0.4, 0.5\}$, скорость обучения $LR \in \{0.001, 0.01, 0.1\}$, функция потерь $LF \in \{\text{MSE}\}$, размер партии $BS \in \{16, 32, 64\}$, количество слоев $LN \in \{5, ..., 9\}$.

Шаг 2. Исходная популяция P_0 создаётся с n индивидуумами. $P_0 = \{I_1, I_2, \ldots, I_n\}$, здесь каждый индивидуум I_n представляет собой настройку гиперпараметров и слоёв ИНС.

$$I_n = \{LR_n, BS_n, DR_n, LF_n, LS_n\},\ LS_n = \{(NE_{n1}, AF_{n1}), \ldots, (NE_{nL}, AF_{nL})\},$$

в данном случае LS – количество слоёв, NE – количество нейронов, AF – функция активации, L – общее число слоёв сети. Значения этих параметров случайно выбираются из набора гиперпараметров, указанных на шаге 1.

Шаг 3. Пригодность каждого индивидуума I оценивается по точности ИНС, созданной на основе гиперпараметров, с использованием функции среднеквадратичной ошибки *(MSE)* на тестовой выборке.

$$f(I_n) = AC_{тест}(M_d(I_n)),$$

здесь $M_d(I_n)$ обозначает ИНС, созданную на основе гиперпараметров I_n, а $AC_{тест}$ представляет точность на контрольной выборке.

Шаг 4. Оператор кроссовера применяется для создания нового потомка I_c - путём кроссовера между двумя родителями I_p (отец) и I_q (мать). Эта операция выполняется для каждого гиперпараметра следующим образом:

$$I_c[g] = \begin{cases} I_p[g], & \textit{если } t_s < 0.5 \\ I_q[g], & \textit{иначе} \end{cases},$$

здесь t_s – это случайное значение из диапазона от 0 до 1. g – это ген, представляющий переменную, соответствующую каждому гиперпараметру.

Шаг 5. Мутация выполняется для каждого выбранного гена g следующим образом: значение $I_n[g] = g'$ заменяется случайным значением, взятым из диапазонов, определённых на шаге 1.

Выбранный гиперпараметр обновляется с применением нового значения, при этом обновляется только выбранный гиперпараметр. Пример: пусть индивидуум I_n - имеет следующие гиперпараметры:

$$I_n = \{LR = 0.01, BS = 32, DR = 0.2, LF = "mse", NL = 5, AF = "relu"\}$$

Если случайно выбранным гиперпараметром при мутации является LR, и новое случайно выбранное значение равно 0.001, то обновлённый индивидуум $I_n^{'}$ будет следующим:

$$I_n^{'} = \{LR = 0.001, BS = 32, DR = 0.2, LF = "mse", NL = 5, AF = "relu"\}$$

Шаг 6. Генетический алгоритм выполняется на протяжении $G=5$ поколений, где в каждом из них отбираются $P=5$ популяций по критерию пригодности и применяются генетические операции для создания следующего поколения. Процесс завершается, предоставляя оптимальные гиперпараметры и наилучшую точность на тестовой выборке.

ИНС для классификации 16-битных шифровальных ключей, основанная на алгоритме **A1**, была обучена с использованием оптимизатора ADAM в течение 10 000 эпох. Значения преобразованы в диапазон от 0 до 1 с помощью

сигмоидной функции активации. Процесс обучения был оптимизирован с использованием библиотеки Keras и её функции Callback, Model Check point и EarlyStopping. В результате точность составила 97,5% на обучающей выборке и 96,2% на контрольной выборке.

Третья глава диссертации, под названием **«Гибридные алгоритмы формирования высоконелинейных подстановочных компонентов»**, посвящена разработке статических и динамических S-компонентов. В данной главе представлен алгоритм гибридного применения генетического алгоритма с тригонометрическими и аффинными подстановками.

В параграфе 3.1 представлен алгоритм формирования динамических нелинейных подстановочных значений с использованием тригонометрической функции в параметрах генетического алгоритма. В качестве тригонометрической функции была выбрана следующая: $f(z)=\sin((A+B)\cdot x\cdot z+C)$, здесь $0<x<1,\ 0\le z\le(2^n-1), B\in z$ и $A,C=\{1,3,...,2^n-1\}$.

В этой функции динамические *S*-компоненты были сгенерированы случайным выбором переменных *A, B, C* и *X* из заданных диапазонов. Компонент S_1 был сформирован на основе тригонометрической функции с высокой стойкостью (*TFOSH*) путём оптимизации параметров *X, A* и *C*.

В параграфе 3.2 разработан алгоритм формирования статических компонентов с высокой нелинейностью с помощью генетических алгоритмов для аффинной функции. Компоненты *S{8×8}* были созданы на основе метода, используемого в AES. Нелинейный компонент AES рассчитывается в поле Галуа $GF(2^8)$ через неприводимый многочлен $m(x)=x^8+x^4+x^3+x+1$ с использованием функции $S(x)=A\cdot x^{-1}+b$, здесь A – бинарная матрица размером 8×8, а b – бинарный вектор длиной 8. Матрица – *A* рассматривается как матрица смежности, описывающая связи графа, и формируется из множеств *V* и *U*. Она является особенной с ненулевым определителем. Алгоритм A_2, который генерирует особенную матрицу смежности с помощью генетического алгоритма, включает следующие шаги.

Входные параметры: n – размер матрицы, m – количество матриц для начальной популяции, μ – вероятность мутации (от 0 до 1), φ – небольшое положительное число для оценки детерминанта, t_{max} – максимальное число поколений, p – точка кроссовера (целое число от 0 до n).

Шаг 1. *Выбор популяции*. Создаётся начальная популяция P_0, состоящая из m матриц смежности, где каждая матрица A_i имеет размер $n\times n$. Каждый элемент A_{ij} в матрице может быть равен либо 0, либо 1.

Шаг 2. Функция пригодности $f(A_i)$ проверяет допустимость матрицы смежности A_i, оценивая, является ли она особенной или неособенной.

$$f(A_i)=\begin{cases}\varphi, & \text{если } \det(A_i)=0\\ \left|\det(A_i)\right|, & \text{иначе}\end{cases}$$

Шаг 3. Выживание A_i определяется с использованием метода рулетки, где вероятность зависит от оценки пригодности и пропорциональна её значению.

$$P_t(A_i)=f(A_i)\Big/\sum_{k=1}^{m} f(A_k)$$

Шаг 4. Для кроссовера случайным образом выбирается точка *p*, и две новые матрицы A_{n1} и A_{n2} создаются путём смешивания элементов исходных (родительских) матриц следующим образом:

$$A_{n1} = \left[A_{p1}[1:p],\ A_{p2}[p+1:n] \right],\quad A_{n2} = \left[A_{p2}[1:p],\ A_{p1}[p+1:n] \right],$$

здесь A_{p1} и A_{p2} — это исходные (родительские) матрицы.

Шаг 5. Каждый элемент матрицы A_{ij} подвергается мутации с вероятностью μ.

$$A'_{ij} = \begin{cases} 1 - A_{ij}, & \mu \text{ с вероятностью} \\ A_{ij}, & \text{иначе} \end{cases}$$

Шаг 6. Новая матрица оценивается с помощью фитнес-функции. Если не найдена особенная матрица или количество поколений достигло t_{max}, алгоритм завершается. В противном случае для формирования новой матрицы следующего поколения A'_{ij} процесс возвращается к шагу 2.

Шаг 7. Если матрица удовлетворяет условию быть особенной матрицей смежности, то матрица размером $n \times n$ принимается в качестве результата, и алгоритм завершается.

Алгоритм использовался для генерации аффинных подстановок, на основе которых формировались статические S-компоненты. Оценка S-компонентов проводилась по следующим критериям: нелинейность *N(f)* и *N(S)*, алгебраический иммунитет *AI(S)*, строгое лавинное свойство *(SAC)*, вероятность линейного приближения *(LP)*, дифференциальная однородность *(DU)*, фиксированные *(FP)* и противоположные фиксированные точки *(OFP)*.

В параграфе 3.3, посвящённом методам формирования динамических S-компонентов с высокой нелинейностью с использованием гибридного подхода, объединяющего генетический алгоритм и параметры аффинных подстановок, на основе экспериментов были выявлены следующие теоремы:

Теорема 1. В алгоритме Rijndael, если общий показатель нелинейности *N(S)* для S-компонента, рассчитанного с помощью неприводимого многочлена *m(x),* матрицы *A* и аффинной подстановки $S(x) = A \cdot x^{-1} + b$, равен 112, то при повороте матрицы *A* по часовой или против часовой стрелки на 90, 180 или 270 градусов, общий показатель нелинейности для полученных S-компонентов также будет равен 112.

Теорема 2. Если в аффинной подстановке значение вектора *b* равно 0,0,0,0,0,0,0,0 или 1,1,1,1,1,1,1,1, то нелинейный *S*-компонент размером 8×8, рассчитанный с использованием подстановки $S(x) = A \cdot x^{-1} + b$, будет иметь как минимум одну фиксированную точку *(FP)* или противоположную фиксированную точку *(OFP).*

На основе свойств приведённых и рассмотренных функций аффинной подстановки была сформирована следующая функция.

$$S(x) = A_{2,r_2}^{d_2} \cdot \left(A_{1,r_1}^{d_1} \cdot x + b_1 \right)^{-1} + b_2$$

Сформированная аффинная функция включает выходное значение *S(x)*, входное *x*, и бинарные матрицы A_1 (1) и A_2 (2) размером 8×8 с параметрами d_1, d_2 (1 или -1), углами r_1, r_2 (0, 90, 180, 270 градусов) и векторами b_1, b_2. Эти параметры создают динамические компоненты *S(x)* из 256 элементов с нелинейностью $N(S)_{min}$=112. Общее количество комбинаций: 2 для d_1 и d_2, 4 для r_1 и r_2, и 254 для b_1 и b_2.

$$S_u = d_1 \times d_2 \times r_1 \times r_2 \times b_1 \times b_2 = 2 \times 2 \times 4 \times 4 \times 254 \times 254 = 4129024$$

Вычисление значений динамических нелинейных подстановок *S{8×8}* выполнялось с использованием генетического алгоритма. В качестве параметров функции были взяты матрицы A_1 и A_2, представленные как (1) и (2), а также неприводимый многочлен $m(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$.

$$A_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (1)$$

$$A_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

Был сформирован нелинейный компонент S_1, созданный с использованием выбранных значений через аффинную функцию (*AFOSH*). Для формирования динамических компонентов *AFOSH* с вышеуказанными параметрами были вычислены компоненты S_2{8×8}, S_3{8×8}, S_4{8×8} и S_5{8×8} с помощью некоторых значений d_1, d_2, r_1 , r_2, b_1, и b_2.

Четвёртая глава диссертации **«Анализ результатов классификации и формирования нелинейных компонентов, а также программного комплекса для их формирования»**, описывает улучшенные алгоритмы и разработанный программный комплекс. Также проведён сравнительный анализ результатов экспериментов с новыми алгоритмами и существующими решениями, а также их практическое применение.

Таблица 1.

Результаты применения ММО в нелинейных компонентах S-AES

Исслед. работа	ММО	КНК	ДКК	МВГ	ОВ	ТКВ
H. Grari и др.(2022)	MLP	ключ шифрования	16	ВСП	2400, 600	0.75
H. Kim и др. (2023)	RESNET		16	ВСП	900000, 500000	0.69
Это исслед.	MLP		48,16	ГА	2048, 512	0.96
Это исслед.	SVM	раундовый ключ	32,48	Optuna	1024, 256	0.88

В параграфе 4.1 проанализированы результаты, полученные методом и алгоритмом классификации ключей с оптимизацией гиперпараметров, и проведено их сравнение с аналогичными исследованиями. В таблице 1

приведён анализ применения методов машинного обучения к нелинейным компонентам S-AES. Обозначения: КНК – классифицированный компонент, ДКК – длина компонента, МВГ – метод подбора гиперпараметров, ОВ – обучающая выборка, ТКВ – точность на контрольной выборке, ВСП – выбор пользователя, ГА – генетический алгоритм. Результаты показали, что метод с использованием SVM повысил точность на 13%, при этом обучающая выборка уменьшилась на 952 элемента.

В параграфе 4.2 рассматриваются структура и функциональные возможности программного комплекса для формирования статических и динамических S-компонентов с использованием генетического алгоритма. Комплекс позволяет создавать высоконелинейные S-компоненты через отбор особенных матриц смежности, а также проверять стойкость существующих $S\{8\times8\}$ компонентов на соответствие криптографическим требованиям.

В параграфе 4.3 проведён сравнительный анализ результатов алгоритмов формирования нелинейных подстановок. Исследование сравнивает стойкость S-компонентов, созданных новыми алгоритмами, с результатами других исследований. Для сбалансированных 8-битных S-компонентов важны следующие значения: $N(S) = 112$, $AI(S) = 3$, $DU(S) = 2$, $SAC(S) = 0.5$, $FP(S) = 0$, $OFP(S) = 0$, $AFP(S) = 0$.

В таблице 2 представлены результаты оценки компонентов $S_1\{8\times8\}$, $S_2\{8\times8\}$ и $S_3\{8\times8\}$, сформированных в параграфе 3.2, и статических S-компонентов других исследователей. Оценка включала: $N(f)_{min}$, $N(f)_{max}$ $N(S)$, LP, DU, SAC, а также сумму фиксированных и противоположных точек (AFP).

Таблица 2.

Оценка статических S-компонентов по критериям устойчивости.

S компонент	**Время объяв.**	$N(f)_{макс}$	$N(f)_{мин}$	$N(S)$	$AI(S)$	LP	DU	$SAC(S)$				AFP
								мин	**мах**	**сред.**	**ср.кв. отк.**	
S_1	2023	112	112	112	2	16	4	0.453	0.547	0.5	0.0276	0
S_2	2023	112	112	112	2	16	4	0.453	0.531	0.5	0.0236	3
S_3	**2024**	**112**	**112**	**112**	**2**	**16**	**4**	**0.453**	**0.531**	**0.5**	**0.0236**	**0**
N.Siddiqui и др. S_7	2020	112	112	112	2	16	4	0.437	0.547	0.496	0.0286	2
Y.Wang и др. S_1	2020	112	94	94	3	32	10	0.425	0.578	0.495	0.0324	3
Y.Wang и др. S_1	2012	108	92	92	3	36	10	0.406	0.578	0.506	0.0380	5
Rinjdael AES	1998	112	112	112	2	16	4	0.453	0.562	0.504	0.0314	0
SM4, Китай	2016	112	112	112	2	16	4	0.437	0.562	0.499	0.0345	1
Кузнечик	2015	116	100	100	3	28	8	0.437	0.609	0.512	0.0387	0
A. Razaq и др S_1	2022	112	96	96	3	34	10	0.453	0.562	0.501	0.0261	4
A. Razaq и др S_1	2023	112	108	108	2	20	6	0.421	0.578	0.501	0.0364	3
M. Ahmad и др S_1	2016	110	92	92	3	36	10	0.406	0.594	0.498	0.0418	1

На основе рассмотренных критериев стойкости и их рекомендованных значений был выполнен расчёт общего показателя стойкости (ОПС) для компонентов $S\{8\times8\}$ по формуле (3). При этом для расчёта среднего значения $SAC_{сред.}$ использовалась формула (4), а для AFP – формула (5).

На основе параметров аффинной функции из параграфа 3.3 были сформированы и проанализированы динамические нелинейные S-компоненты с использованием аффинного замещения и ГА на соответствие критериям стойкости. Сравнительные результаты представлены в таблице 3.

$$ОПС = \left(\frac{N(f)_{мин}}{112} + \frac{N(f)_{макс}}{120} + \frac{N(S)}{112} + \frac{AI(S)}{3} + \frac{258 - DU}{256} + \right.$$
$$\left. + \frac{SAC_{мин}}{0.5} + \frac{1 - SAC_{макс}}{0.5} + \frac{SAC_{сред}}{0.5} + \frac{0.02}{SAC_{сред.кв.отк.}} + AFP \right) / 10 \qquad (3)$$

$$SAC_{сред.} = \begin{cases} \frac{0.5}{SAC_{o'rt}}, если\ SAC_{сред.} > 0.5 \\ 1,\ если\ SAC_{сред.} = 0.5 \\ \frac{1 - SAC_{сред.}}{0.5}, иначе. \end{cases} \qquad (4)$$

$$AFP = \begin{cases} 1 - AFP / 5,\ если\ 5 >= AFP, \\ 0,\ иначе. \end{cases} \qquad (5)$$

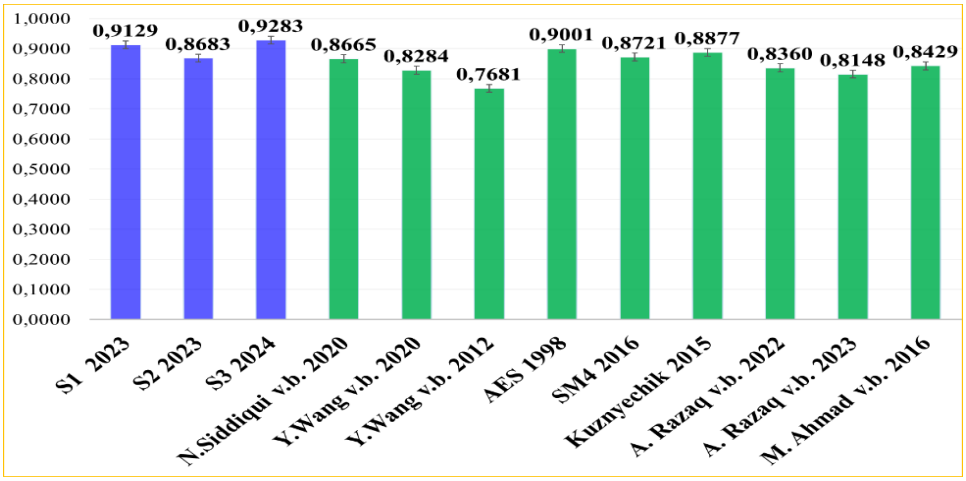


Рис. 2. Указатели ОПС статических S-компонентов

Таблица 3.

Оценка криптографических критериев динамических S-компонентов

***S* компонент**	**Время объяв.**	***N(f)макс***	***N(f)мин***	***N(S)***	***AI(S)***	***LP***	***DU***	***SAC(S)***				***AFP***
								мин	**мах**	**сред.**	**ср.кв. отк.**	
TFOSH S_1	2023	112	94	94	3	34	10	0.391	0.578	0.494	0.044	1
AFOSH S_1	**2024**	**112**	**112**	**112**	**2**	**16**	**4**	**0.453**	**0.547**	**0.5**	**0.027**	**0**
AFOSH S_2	2024	112	112	112	2	16	4	0.437	0.562	0.499	0.030	0
C.B.Erendira и др.	2023	110	96	96	2	32	12	0.391	0.594	0.501	0.043	1
УзГОСТ.1105:2009	2014	108	92	92	3	36	10	0.375	0.625	0.496	0.046	0
A.H.Zahid и др.	2021	112	96	96	3	32	10	0.437	0.562	0.506	0.033	1
K.Abdullah и др.	2021	112	96	96	3	32	12	0.391	0.578	0.496	0.039	5
A.H.Zahid и др.	2020	110	92	93	3	36	10	0.406	0.594	0.498	0.042	2
S.Hussain и др.	2020	110	96	96	3	28	12	0.422	0.631	0.511	0.038	1

S-компонент был оценён по статистическим критериям, таким как энтропия *(H)*, контраст *(K)*, корреляция *(ρ)*, гомогенность *(G)*, энергия *(E)* и среднее абсолютное отклонение *(CAO)*, которые измеряют диффузию и

случайность между входными и выходными значениями пикселей. В исследовании использовались изображения размером 256×256, включая «Лену», «Обезьяну» и «Болгарский перец», часто применяемые в других работах. Каждое изображение преобразовывалось в градации серого и пропускалось через S-компонент, после чего создавалось новое изображение того же размера. Далее результаты оценивались по вышеуказанным критериям для каждого изображения. Для изображения «Лена» результаты представлены в таблице 4. Затем, на основе полученных данных, изображение «Лена» пропускалось через статический компонент S_3, и на рисунке 3 показаны результирующее изображение, его гистограмма и графики автокорреляции соседних пикселей, что позволяет оценить эффективность S-компонента.

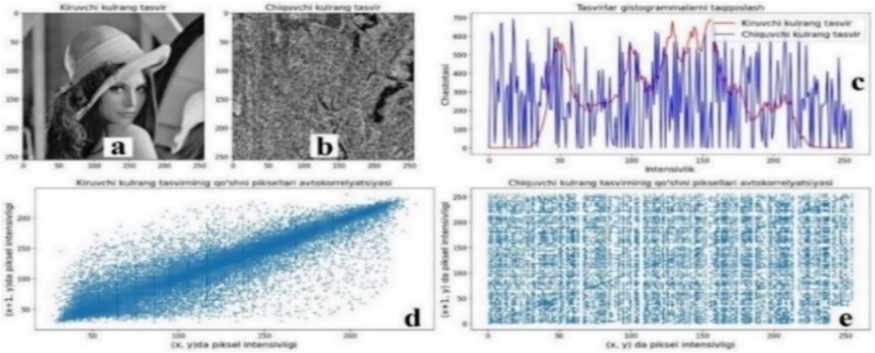


Рис. 3. Изображение «Лена»: (a) исходное изображение, (b) изображение, полученное после обработки через компонент S3, (c) их гистограмма, а также графики автокорреляции соседних пикселей - (d) и (e)

Таблица 4.

Результаты оценки S-компонентов по логическим критериям для изображения «Лена»

S-компонент	*H*	*K*	*ρ*	*E*	*G*	*CAO*
Изображения «Лена»	7.423	256.21	0.9428	0.0183	0.2193	-
Это исслед., стат. S_3	7.423	9563.15	0.0994	0.0183	0.0988	**135.85**
Динам. AFOSH S_1	7.423	10768.38	0.0760	0.0183	0.0972	124.21
AES, США	7.423	10968.52	0.0751	0.0183	0.0968	116.25
SM4, Китай	7.423	9572.14	0.1194	0.0183	0.0976	131.95
Кузнечик, Россия	7.423	9647.07	0.1020	0.0183	0.0990	130.85
УзГОСТ.1105:2009	7.423	9850.39	0.0520	0.0183	0.0966	132.80
Y.Wang и др. S_1	7.423	9533.94	0.0923	0.0183	0.0969	130.36

Сравнение результатов (см. таблицы 2-4) показало, что предложенные методы и алгоритмы превзошли другие подходы, улучшив точность классификации ключей S-AES в среднем на 13%. Статические S-компоненты показали устойчивость по ОПК на 8,2% выше, а динамические — на 6,8% выше. В статистических критериях для изображения «Лена» статический компонент S_3 продемонстрировал значение CAO на 3,05 до 19,6 выше других. Исследование подтвердило эффективность предложенных алгоритмов.

В приложениях к диссертации представлены копии документов, подтверждающих практическое применение результатов исследования, а также копии свидетельств о государственной регистрации программ,

выданных Агентством интеллектуальной собственности при Министерстве юстиции Республики Узбекистан.

ЗАКЛЮЧЕНИЕ

Основные результаты диссертационного исследования на тему «Алгоритмы формирования и классификации нелинейных компонентов» заключаются в следующем:

1. Были исследованы вопросы классификации и формирования нелинейных компонентов симметричных шифровальных алгоритмов, для которых требуется высокая нелинейность, в частности, ключевых битов и нелинейных S-компонентов. В результате анализа были выявлены методы и алгоритмы применения машинного обучения и генетических алгоритмов к нелинейным компонентам блочных шифров с симметричным ключом.

2. Для классификации основных и раундовых битов ключа упрощенного симметричного шифрования S-AES предложен подход формирования обучающих и контрольных выборок на основе выбранного открытого текста, S-компоненты и зашифрованного текста. Данный подход позволяет эффективно классифицировать биты ключа алгоритма S-AES.

3. С помощью Optuna были оптимизированы гиперпараметры для SVM, и разработан ГА для построения архитектуры ИНС. Это позволило повысить контрольную точность на 13% при использовании обучающей выборки, меньшей на 952 элемента, по сравнению с предыдущими исследованиями.

4. С помощью генетического алгоритма была выбрана невырожденная матрицы – *A* и применена для аффинного преобразования, в результате чего была сформирована статическая S_3-компонента. S_3-компонента показала, что ее общая устойчивость на 2,8% выше, чем у стандарта AES США, на 4% выше, чем у алгоритма Кузнечика Российской Федерации, и на 5,6% выше, чем у стандартов шифрования SM4 Китая, по сравнению с исследованиями, проведенными в 1998-2023 годах.

5. В исследовании был предложен алгоритм формирования динамических S-компонент с учетом криптографической оценки параметров генетического алгоритма. Этот алгоритм позволяет создавать динамические S-компоненты с высокой устойчивостью. Результаты исследования показали, что по сравнению с динамической S-компонентой, используемой в стандарте шифрования УзГОСТ 1105:2009, общая нелинейность $N(S)$ увеличилась на 16-20, а общий показатель устойчивости улучшился на 7%. Кроме того, по сравнению с другими S-компонентами был достигнут прирост общего показателя устойчивости на 6,8%.

6. Предложенный в исследовании алгоритм оптимизации гиперпараметров позволяет решать задачи классификации с использованием метода многослойной перцептронной нейронной сети.

7. Программное обеспечение, разработанное на основе алгоритма формирования статических и динамических S-компонентов, можно использовать при проектировании стандартов симметричных шифровальных алгоритмов. Это позволяет повысить устойчивость алгоритмов симметричного шифрования к различным методам криптоанализа.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.03/26.05.2022.T.10.05 AT THE NATIONAL RESEARCH UNIVERSITY "TASHKENT INSTITUTE OF IRRIGATION AND AGRICULTURAL MECHANIZATION ENGINEERS"

RESEARCH INSTITUTE FOR DEVELOPMENT OF DIGITAL TECHNOLOGIES AND ARTIFICAL INTELLIGENCE

ABDURAZZOKOV JAVOKHIR RUSTAMOVICH

ALGORITHMS FOR THE FORMATION AND CLASSIFICATION OF NONLINEAR COMPONENTS

05.01.03 – "Theoretical bases of informatics"

DISSERTATION ABSTRACT
of doctor of philosophy (PhD) on technical sciences

Tashkent – 2024

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme Attestation Commission at the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan under number B2024.1.PhD/T4410.

The dissertation has been prepared at Digital Technologies and Artificial Intelligence Research Institute.

The abstract of dissertation is posted in Three languages (Uzbek, Russian, English (resume)) is placed on the web-page of Scientific Council (www.tiiame.uz) and Information and Educational Portal «Ziyonet» (www.ziyonet.uz).

Scientific adviser:	**Abdurakhimov Bakhtiyor Fayziyevich** doctor of Physical and Mathematical Sciences, Professor
Official opponents:	**Mirzaev Nomaz** doctor of Technical Sciences, Professor
	Xodiev Shukhrat Ilkhamovich candidate of Technical Sciences
Leading organization:	**Samarkand state unversity named after Sharof Rashidov**

Defense of dissertation will take place in «22» november 2024 at 14⁰⁰ o'clock at a meeting of the scientific council DSc.03/26.05.2022.T.10.05 at the National research university «Tashkent institute of irrigation and agriculture mechanization engineers» (Address: 100000, Tashkent, str. Kari Niyazi 39, tel.: (99871) 237-19-36; fax: (99871) 237-54-79; e-mail: admin@tiiame.uz).

The dissertation could be reviewed at the Information-resource center the National research university «Tashkent institute of irrigation and agriculture mechanization engineers» (registration number №342). Address: 100000, Tashkent, str. Kari Niyazi 39, tel: (99871) 237-19-45).

Abstract of dissertation sent out on «12» 11 2024 year.

(mailing report № 7, on «11» 11 2024 year).

N.S. Mamatov
Chairman of Scientific council
on awarding scientific degrees,
doctor of Technical Sciences, Professor

D.K. Bekmuratov
Scientific secretary of Scientific council
on awarding scientific degrees,
doctor of philosophy (PhD) on Technical Sciences

S.S. Radjabov
Chairman of the scientific seminar at the
Scientific council on awarding scientific degrees,
doctor of Technical Sciences, Senior researcher

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to develop algorithms for classifying and forming highly nonlinear components of symmetric block ciphers using machine learning and genetic algorithms.

The object of the research work is the processes of classifying and forming nonlinear components of symmetric block encryption algorithms.

The scientific novelty of the research work is as follows:

the approach for forming training and testing datasets based on the nonlinear components of symmetric encryption algorithms has been proposed;

the approach to improving the accuracy of round key classification by optimizing the hyperparameters of the support vector method has been proposed;

the algorithm for classifying encryption key bits based on the application of a genetic algorithm within a neural network architecture has been developed;

the algorithm for generating static nonlinear component values based on extracting a specific adjacency matrix using a genetic algorithm and applying it in an affine function has been developed;

the algorithm for generating dynamic nonlinear component values considering cryptographic evaluation in the parameters of the genetic algorithm has been developed.

Scientific and practical significance of the research results. The scientific significance of the obtained results is explained by the improved accuracy of key bit classification in symmetric block encryption algorithms through the selection of support vector methods and neural network hyperparameters using modern optimization techniques and genetic algorithms, as well as by achieving high resilience in the results of algorithms for forming nonlinear S-components.

The practical significance of the research results lies in the fact that the developed algorithms and software can be applied to the classification of nonlinear data and in the round functions of modern symmetric block ciphers.

Implementation of the research results. Based on the developed algorithms and software suite for forming and classifying nonlinear components in the research:

the classification algorithm, developed by optimizing neural network hyperparameters based on genetic algorithms was implemented in the practical activities of the Digitization and Data Storage Center of the Surkhandarya Regional Statistics Department (certificate of the Khokimiyat of the Surkhandarya region No. 07-07/1988 dated September 23, 2024). As a result, the developed algorithm improved the forecasting of economic indicators by 8-10% and reduced processing time by 11-13%;

in the research, a software was developed by substituting the S-component, formed based on the genetic algorithm, for the internal nonlinear substitution block of AES. This software was implemented at the regional branch of the Ministry of Digital Technologies in Surkhandarya for encrypting large-scale data (certificate of the Khokimiyat of the Surkhandarya region No. 07-07/1988 dated September 23, 2024). As a result, after inputting 100,000 random plaintexts and keys, the encryption time for plaintexts was reduced by 11.5-12.5%, and decryption time

decreased by 10.5-12% compared to the existing AES algorithm;

the proposed static nonlinear S-component was experimentally tested at the “Center for the Development of Information and Communication Technologies” LLC, under the State Assets Management Agency of Surkhandarya Region, for ensuring reliable protection, encryption, and security assessment of data in wireless local networks (certificate of the Khokimiyat of Surkhandarya region No. 07-07/1988 dated September 23, 2024). The results showed that the resilience of the S-component was approximately 12.5% higher compared to the existing nonlinear substitution blocks of AES;

in order to ensure the security of a wireless local network and to evaluate the efficiency of data encryption, a static S nonlinear component developed within the research was implemented in the information exchange process at the "Center for the Development of Information and Communication Technologies" LLC, under the Surkhandarya Regional Department of State Assets Management (certificate of the Khokimiyat of the Surkhandarya region No. 07-07/1988 dated September 23, 2024). As a result, the static S component achieved an average 12.5% higher performance in overall robustness compared to the internal nonlinear substitution block of the AES encryption standard;

the software suite developed based on the S component formulated in the research was implemented at the IT Park Termez branch in Surkhandarya region for the purpose of securing large volumes of data (certificate of the Khokimiyat of the Surkhandarya region No. 07-07/1988 dated September 23, 2024). As a result, by inputting one million random plaintexts and keys, the generated ciphertexts demonstrated a 13-15% reduction in processing time compared to the AES algorithm;

the proposed static nonlinear S scomponent was experimentally tested at the “Center for the Development of Information and Communication Technologies” LLC, under the State Assets Management Agency of Surkhandarya Region, for ensuring reliable protection, encryption, and security assessment of data in wireless local networks (certificate of the Khokimiyat of the Surkhandarya region No. 07-07/1988 dated September 23, 2024). The results showed that the resilience of the S-component was approximately 12.5% higher compared to the existing nonlinear substitution blocks of AES;

the static S-component formed based on the genetic algorithm was implemented in place of the S-component of China's SM4 encryption algorithm at China's Inner Mongolia Wangxin Information Security Service Co., Ltd. (Reference No. WXSEC20240410005 dated April 10, 2024, issued by Inner Mongolia Wangxin Information Security Service Co., Ltd). As a result, the resilience of the SM4 encryption algorithm improved by an average of 13-13.5%.

Structure and volume of the dissertation. The dissertation consists of an introduction, four chapters, conclusion, the list of used literature and appendix. The volume of the dissertation is 120 pages.

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

I bo‘lim (I часть; I part)

1. 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. – Switzerland, 2024. – Vol. 718. – Pp. 113-121. – DOI:10.1007/978-3-031-51521-7_16. (№3 ; Scopus Q4, SJR 2023=0.17)

2. Abduraximov B.F, Abdurazzoqov J.R. Soddalashtirilgan AESning kaliti haqida ma’lumotga ega bo‘lish maqsadida chuqur o‘qitishga asoslangan kriptotahlildan foydalanish // Informatika va energetika muammolari O‘zbekiston jurnali. – Toshkent, 2023. –№ 2. –B. 17-26. (05.00.00; №5)

3. Abdurazzokov J. S-Box Generation Algorithm by Constructing the Non-Singular Adjacency Matrix Using the Genetic Algorithm // American Journal of Science, Engineering and Technology. – New York, 2024 – Vol. 9, Issue 1. – Pp. 14-20. – DOI: 10.11648/j.ajset.20240901.12. (05.00.00; №28)

4. 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). – Tashkent, 2022. – Pp. 1-5. – DOI: 10.1109/ICISCT55600.2022.10146796. (№3; Scopus)

5. Abdurazzokov J. Algorithm for Generation of S-box Using Trigonometric Transformation in Genetic Algorithm Parameters // Chemical Technology Control and Management. – Tashkent, 2023. – Vol. 111, Issue 3. – Pp 69-75. (05.00.00; №12)

6. Abdurazzokov J. Dynamic S-Box Generation Algorithm with Improved Strict Avalanche Criterion by Selection of Adjacency Matrix Parameters // 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS). – Tashkent, 2023. – Pp. 393-398. – DOI: 10.1109/ICTACS59847.2023.10389847. (№3; Scopus)

7. Abdurazzoqov J.R. Orgraf parametrlarini tanlash orqali yuqori nochiziqli, yaxshilangan qat’iy lavin samaradorligiga ega S-bloklarni hisoblash algoritmi // Ilm-fan va innovatsion rivojlanish ilmiy-texnikaviy jurnali. – Toshkent, 2023. – № 5. – B. 42-53. (05.00.00; OAK Rayosatining 2019-yil 28-fevraldagi 262/9.2-son qarori)

8. Abduraximov B.F., Abdurazzoqov J.R. Simmetrik shifrlash algoritmlariga bardoshli S-blokni qo‘shnilik matritsasi parametrlarini tanlash orqali generatsiya qilish algoritmi // Farg‘ona politexnika instituti ilmiy - texnika jurnali. – Farg‘ona, 2023. – № 5. – B. 136-146. (05.00.00; №20)

9. 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). – Palembang (Indonesia), 2023. – Pp. 372-377. – DOI:

10.1109/EECSI59885.2023.10295947. (№3; Scopus)

10. Abdurazzokov J. Simplified AES Key Bits Classification using Machine Learning Techniques // International Journal of Advanced Research in Science, Engineering And Technology. – India, 2023. – Vol. 10, Issue 12. – Pp. 21339-21346. (05.00.00; №8)

11. Abdurazzokov J., Turaev R., Abdurazzokov I. Using Deep Learning Cryptanalysis to Derive Data About Simplified AES Keys // 2023 International Conference on Information Science and Communications Technologies (ICISCT). – Tashkent, 2023. –Pp. 281-285. (05.00.00; OAK Rayosatining 2023-yil 29-avgustdagi 342/3-son qarori)

12. Abdurazzokov J. Algorithm for Generating S-box Using Trigonometric Function // 2023 International Conference on Information Science and Communications Technologies (ICISCT). –Tashkent, 2023. – Pp. 585-589. (05.00.00; OAK Rayosatining 2023-yil 29-avgustdagi 342/3-son qarori)

II bo‘lim (II часть; II part)

13. Abdurakhimov B.F, Boykuziev I.M., Abdurazzokov J.R. Encryption systems and the history of their development // Proceedings of the 2nd International Scientific and Practical Conference Scientific Goals and Purposes in XXI century. – Seattle, USA 19-20.01.2022. –P.p.768-776. –DOI:10.51582/interconf.19-20.01.2022.085.

14. Abdurazzoqov J.R. Sun’iy intellektning rivojlanishi va uning axborot xavfsizligida foydalanish istiqbollari // O‘zbekiston Respublikasi Ichki ishlar vazirligi Akademiyasida Kibermakonda sodir etilayotgan jinoyatlarga qarshi kurash: muammolar va yechimlar Respublika ilmiy-amaliy konferensiya materiallari to‘plami. –Toshkent, 24-fevral 2022-yil. –B. 339-343.

15. Abdurazzoqov J. Feystel tarmog‘i va uning asosida qurilgan shifrlash algoritmlari tahlili // “Fan, ta’lim va texnikani innovatsion rivojlantirish masalalari” nomli Xalqaro ilmiy-amaliy onlayn anjumani ma’ruzalar to‘plami. –Andijon, 12-aprel 2022-yil. –B. 61-65.

16. Abdurazzoqov J. Simmetrik blokli shifrlash algoritmlari S-bloki qiymatlarini genetik algoritmlar yordamida generatsiya qilish usullarini tahlil qilish // “Matematik modellashtirish va axborot texnologiyalarining dolzarb masalalari” mavzusida xalqaro ilmiy-amaliy anjumani ma’ruzalar to‘plami. –Nukus, 2-3-may 2023-yil. –B. 171-173.

17. Abdurazzoqov J. Simmetrik blokli shifrlash algoritmlariga bardoshli S-bloklarni generatsiya qilish muammolari // “Raqamli texnologiyalar: sohalarda amaliy joriy etishning yechimlari va muammolari” nomli Xalqaro qo‘shma ilmiy-texnik anjumani ma’ruzalar to‘plami. – Toshkent, 27-28-aprel 2023-yil. –B. 568-571.

18. Abduraximov B.F, Abdurazzoqov J.R. Genetik algoritmlar yordamida simmetrik shifrlash algoritmlarining nochiziq S-komponentni shakllantirish muammolari tahlili // “Ta’lim jarayoniga raqamli texnologiyalar va sun’iy intellektni joriy etish istiqbollari” mavzusida resublika ilmiy-amaliy konferensiya ma’ruzalar

to‘plami. –Termiz, 7-iyun 2024-yil. –B. 314-316.

19. Abduraximov B.F, Abdurazzoqov J.R. Soddalangan AES (S-AES) algoritmining kaliti haqida ma’lumot olish uchun chuqur o‘rganishga asoslangan kriptotahlildan foydalanish algoritmi // O‘zR Adliya vazirligi, O‘zR Dasturiy mahsulotlar davlat reyisterida 04.05.2023-yilda ro‘yxatdan o‘tgan Guvohnoma № DGU 25457.

20. Abduraximov B.F, Abdurazzoqov J.R. Genetik algoritm yordamida orgraf parametrlarini tanlash orqali chiziqsizligi yuqori yaxshilangan qat’iy lavin samaradorligiga ega nochiziq akslantirish blokini hisoblash algoritmi // O‘zR Adliya vazirligi, O‘zR Dasturiy mahsulotlar davlat reyisterida 11.11.2023-yilda ro‘yxatdan o‘tgan Guvohnoma № DGU 29441.

21. Abdurazzoqov J.R. Sun’iy neyron tarmoq giperparametrlarni genetik algoritm yordamida optimallashtirish orqali S-AES kalitlarini tasniflash algoritmi dasturi // O‘zR Adliya vazirligi, O‘zR Dasturiy mahsulotlar davlat reyisterida 13.12.2023-yilda ro‘yxatdan o‘tgan Guvohnoma № DGU 31518.

Avtoreferat TDPU «Ilmiy axborotlari» jurnali tahririyati

tomonidan 2024-yil 17-oktabr tahrirdan o‘tkazildi.

Bosishga ruxsat etildi: 18.10.2024 yil
Bichimi 60x84 $^{1}/_{16}$, «Times New Roman»
garniturada raqamli bosma usulida bosildi.
Nashriyot bosma tabog‘i 3.0. Adadi: 100. Buyurtma: № 27
Bahosi kelishuv asosida

Nizomiy nomidagi Toshkent davlat pedagogika
universiteti bosmaxonasida chop etildi.
Manzil: Toshkent shahar, Chilonzor tumani,
Bunyodkor ko‘chasi 27-uy.