O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.12.2019.FM.01.02 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY UNIVERSITETI

LIU LINGYUN

KRIPTOTAHLIL USULLARI YORDAMIDA SM4 SHIFRLASH ALGORITMINI BAHOLASH

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

FIZIKA-MATEMATIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

UDC: 004.056.55

Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati mundarijasi

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

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

O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.12.2019.FM.01.02 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY UNIVERSITETI

LIU LINGYUN

KRIPTOTAHLIL USULLARI YORDAMIDA SM4 SHIFRLASH ALGORITMINI BAHOLASH

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

FIZIKA-MATEMATIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent-2024

Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2023.4.PhD/FM991 raqam bilan ro‘yxatga olingan.

Dissertatsiya O‘zbekiston milliy universitetida bajarilgan.

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

Ilmiy rahbar:	**Abduraximov Baxtiyor Fayzievich** fizika-matematika fanlari doktori, professor
Rasmiy opponentlar:	**Kabulov Anvar Vasilovich** fizika-matematika fanlari doktori, professor
	Nie Yang PhD, professor, Jining Pedagogika universiteti, Xitoy
Yetakchi tashkilot:	**Termiz davlat universiteti**

Dissertatsiya himoyasi O‘zbekiston milliy universiteti huzuridagi DSc.03/30.12.2019.FM.01.02 raqamli Ilmiy kengashning 2024-yil “29” avgust soat __ dagi majlisida bo‘lib o‘tadi. (Manzil: 100174, Toshkent shahri, Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (99871) 227-12-24, faks: (99871) 246-53-21, e-mail: nauka@nuu.uz).

Dissertatsiya bilan Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (78 - raqam bilan ro‘yxatga olingan). (Toshkent shahri, Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (99871) 246-02-24).

Dissertatsiya avtoreferati 2024-yil “16” avgust da tarqatildi.
(2024-yil “24” iyun dagi 3 raqamli reestr bayonnomasi.)

M.M.Aripov
Ilmiy darajalar beruvchi ilmiykengash raisi, f.-m.f.d.,

Z.R.Rakhmonov
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, f.-m.f.d.

A.V.Kabulov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi, t.f.d., professor

KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon miqyosida axborotning maxfiyligini ta’minlashda keng foydalaniladigan simmetrik blokli shifrlash algoritmlarining kriptotahlil usullariga bardoshliligini baholash masalalariga, jumladan, maxfiy kalitni aniqlashga qaratilgan va algoritm tarkibidagi matematik akslantirishlarning xususiyatlariga, algoritmning qadamlari ketma-ketligiga bog‘liq ravishda, shuningdek akslantirishlarning matematik xususiyatlari hamda algoritmning qadamlariga bog‘liq bo‘lmagan tarzda o‘tkaziladigan kriptotahlil usullariga baholash masalalariga alohida ahamiyat berilmoqda. Akslantirishlarning matematik hususiyatlarini tahlil qilish, algoritmlarni mavjud kriptotahlil usullariga nisbatan baholash masalalari kriptografiya, kriptotahlil va axborot xavfsizligi kabi sohalarda olib borilayotgan ilmiy tadqiqotlarning obyekti hisoblanadi. Shu sababli, fan sohalari va texnologiya yutuqlari rivojlanishining tezkorligini inobatga olgan holda shifrlash algoritmlarini kriptotahlil usullariga nisbatan bardoshlilik talablari bo‘yicha doimiy baholab borish muhim vazifalardan biri bo‘lib qolmoqda.

Hozirgi kunda jahonda axborot xavfsizligini ta’minlash dasturiy va apparat-dasturiy vositalardan foydalangan holda amalga oshiriladi, shu sababli mazkur vositalarda foydalanilgan standart kriptografik shifrlash algoritmlari va protokollar kriptotahlil usullariga bardoshlilik talablari bo‘yicha keng tadqiq etilmoqda. Simmetrik shifrlash algoritmlaridan axborotlarni saqlash, qayta ishlash, uzatish jarayonida maxfiylikni ta’minlashda keng miqyosda foydalaniladi. Shuningdek, SM4 simmetrik blokli shifrlash algoritmi hisoblash tezligi uchun apparat strukturasini loyihalash va optimallashtirishga hamda bardoshliligini aniqlash muhim ahamiyat kasb etadi. Shu sababdan standart simmetrik shifrlash algoritmlarini tahlil qilish va zamonaviy kriptotahlil usullariga bardoshliligini uzluksiz ravishda baholab borish maqsadli ilmiy tadqiqotlardan hisoblanadi.

O‘zbekiston Respublikasida fundamental fanlarning ilmiy va amaliy tatbiqi sifatida axborot xavfsizligi, kriptologiya sohalarida bardoshli kriptografik algoritmlarni yaratish, ularning xavfsizligini baholash kabi dolzarb yo‘nalishlarga katta e’tibor qaratilmoqda. Axborotning maxfiyligini va butunligini ta’minlashda simmetrik blokli shifrlash algoritmlaridan foydalanishga, simmetrik blokli shifrlash algoritmlarini kriptotahlil usullariga baholashga qaratilgan usul va algoritmlarni yaratishga hamda qo‘llashga oid salmoqli natijalarga erishilmoqda. “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlarida, jumladan “idoraviy raqamli infratuzilmaning axborot xavfsizligini, shuningdek, elektron ma’lumotlar va hujjatlarning himoyasini ta’minlash»[1] bo‘yicha vazifalar belgilangan. Ushbu vazifalarni amalga oshirishda standart shifrlash algoritmlarini kriptotahlil usullariga baholash hamda olingan natijalarni amaliyotga joriy qilish muhim ahamiyatga ega.

[1] O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-sonli Farmoni

O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son “2022-2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida” gi farmoni, 2020-yil 7-maydagi PQ-4708-son “Matematika sohasidagi ta’lim sifatini oshirish va ilmiy-tadqiqotlarni rivojlantirish chora-tadbirlari to‘g‘risida”gi qarori, 2019-yil 8-oktabrdagi PF-5847-son “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi farmoni, 2019-yil 27-apreldagi PQ-3682-son “Innovatsion g‘oyalar, texnologiyalar va loyihalarni amaliyotga joriy qilish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori va 2021-yil 1-apreldagi PF-6198-son “Ilmiy va innovatsion faoliyatni rivojlantirish bo‘yicha davlat boshqaruvi tizimini takomillashtirish to‘g‘risida”gi farmonlari, hamda mazkur faoliyatga tegishli boshqa normativ-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

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

Muammoning o‘rganilganlik darajasi. Simmetrik blokli shifrlash algoritmlarini kriptotahlillash va bardoshli simmetrik blokli shifrlarni yaratish masalalari bo‘yicha ko‘plab olimlar ilmiy izlanishlar olib borishgan. Jumladan, Ji W., Hu L., Schneier B., Liu F., Ferguson N., Knudsen L., Hang W., Huili C., Xiaoqing L. V., Dodis Y., Matsui M., Kim T., Courtois N., Zhang W., Harris N., Shamir A., Su B.Z., Wu W.L., Bigham E., Kelsey J., Cho J., Jakimoski G., Oleynikov R., Sun Y. Ishchukova E., Hu W., Babenko L., Shan W., Kazimirov O. va boshqalar tomonidan shifrlash algoritmi va bardoshli kriptografik akslantirishlarni ishlab chiqish hamda ularni kriptotahlil usullariga baholash bo‘yicha ilmiy-tadqiqotlar olib borilgan.

Jahon miqyosida, ko‘plab kriptograflar va kriptotahlilchilar tomonidan SM4 algoritmiga nisbatan ko‘plab kriptoanalitik tadqiqotlar o‘tkazilgan. Jumladan, Kim T. va boshqalar tomonidan 22 raundli qisqartirilgan SMS4 algoritmiga chiziqli hujum va differentsial hujum, 18 raundlik qisqartirilgan SMS4 algoritmiga nisbatan bumerang va kavdrat hujumlari amalga oshirishgan. SM4 algoritmini Vang va Du va boshqalar tomonidan dastlab tanlangan ochiq matnli kuch hujumiga baholashgan. Keyinchalik, Shan va Chen va boshqalar SM4 da o‘z qamrovini kengaytirish uchun maxsus ochiq matnlardan foydalangan holda ushbu hujumni kengaytirdi. Quvvatni tahlil qilishda korrelyatsiyani kuchaytirishga intilishda Xu va boshqalar keng qamrovli adaptiv tanlangan ochiq matnli yondashuvni SM4 algoritmiga nisbatan taklif qilgan. Maamar O va boshqalar tomonidan moslashuvchan bo‘lmagan va moslashuvchan senariylarda qo‘llash uchun texnikani yanada takomillashtirish metodologiyasi asosida SM4 va AES kabi turli algoritmlar baholangan.

Chjan va boshqalar baytga yo‘naltirilgan tasodifiy xato modelini qo‘llashgan, mazkur hujum differentsial tahlil usullarini o‘z ichiga olganb. Hujum usuli nazariy jihatdan SM4 ning 128 bitli asosiy kalitini to‘liq tiklash uchun faqat 32 ta noto‘g‘ri shifrlangan matnni talab qiladi. Hu va boshqalar ma’lumotlar sizib chiqishi mumkin

bo‘lgan bir nechta joylarga hujum qilish orqali ma’lumotlarning sizib chiqish nuqtasi muvaffaqiyatli topilgan va keyinchalik 128 bitli shifrlash kalitini aniqlashda foydalaniladigan 1, 2, 3 va 4-raundlar uchun kalitlar muvaffaqiyatli tiklangan. Vang S. va boshqalar quvvatni modellashtirish uchun Hamming masofasi modeli va bit modelidan foydalangan. WANG M. va boshqalar tomonidan oraliq ma’lumotlar sifatida so‘ralgan chiqishdan foydalangan holda SMS4 ga qarshi tanlangan oddiy matn quvvatini tahlil qilish hujumini taklif qilingan. Shan W. va boshqalar SM4 blok shifriga qarshi CPA tanlangan ochiq matn usulini qo‘llagan. Jiazhe C. va boshqalarning ochiq matnning adaptiv tanloviga asoslangan DPA hujumi, SM4 ning chiziqli transformatsiyasida o‘zgaruvchan kirish bitlarining chiqish bitlariga ta’sirini minimallashtirgan, bu esa SM4 ga samarali yon kanal hujumini ta’minlagan. Hu W. va boshqalar tomonidan shifr izlarini olish jarayoni ikki bosqichga ajratilgan. Yuqori signal-shovqin nisbati izlariga mos keladigan maxsus ochiq matnlarning moslashtirilgan tanlovi hujumni kamroq izlar bilan yakunlashga imkon bergan. Heuser A. va boshqalar tomonidan chiqishlarni modellashtirishni matematik usullar bilan ma’lum darajada kamaytirish mumkinligi ko‘rsatilgan. Hozirgi vaqtda SM4 dasturiy ta’minotini amalga oshirish usullari bo‘yicha ko‘p tadqiqotlar mavjud emas. Ko‘plab tadqiqotchilar SM4 algoritmining apparatni amalga oshirish strukturasini o‘rgangan bo‘lsalarda, tadqiqotlarning ko‘pchilik qismi SM4 algoritmining hisoblash tezligi uchun apparat strukturasini loyihalash va optimallashtirishga e’tibor qaratilgan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti O‘zbekiston Milliy universitetining ilmiy-tadqiqot ishlari rejasiga muvofiq UZB-Ind-2021-98 raqamli “Oqimli shifrlash algoritmlarini tadqiq qilish va ishlab chiqish” mavzusidagi loyiha doirasida bajarilgan.

Tadqiqot ishining maqsadi SM4 simmetrik shifrlash algoritmi va uning modifikatsiya varianti SM4_Mixning bardoshliligini kriptotahlil usullari yordamida baholash va dasturiy hamda apparat ko‘rinishda amalga oshirishning optimal usullarini aniqlashdan iborat.

Tadqiqotning vazifalari:

SM4 simmetrik blokli shifrlash algoritmining bardoshliligini chiziqli kriptotahlil usuli yordamida baholash;

SM4 simmetrik blokli shifrlash algoritmining modifikatsiya varianti SM4_Mix algoritmlarining bardoshliligini chiziqli kriptotahlil usuli yordamida baholash;

SM4 simmetrik blokli shifrlash algoritmi va uning modifikatsiya varianti SM4_Mix algoritmlarining bardoshliligini algebraik kriptotahlil usuli yordamida baholash;

SM4 simmetrik blokli shifrlash algoritmi va modifikatsiya varianti SM4_Mix algoritmlarining bardoshliligini tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usuli yordamida baholash;

SM4 simmetrik blokli shifrlash algoritmi va uning modifikatsiya varianti SM4_Mix algoritmlarini dasturiy hamda apparat ko‘rinishda amalga oshirishning optimal usullarini aniqlash.

Tadqiqotning ob’ekti: simmetrik shifrlash algoritmi va kriptoanaliz jarayonlari.

Tadqiqotning predmeti SM4 simmetrik shifrlash algoritmi hamda uning modifikatsiya qilingan varianti SM4_Mix algoritmi va kriptotahlil usullari yordamida baholash usullari.

Tadqiqotning usullari. Tadqiqot jarayonida amaliy kriptografiya va kriptoanaliz usullari, sonlar nazariyasi, ehtimollar nazariyasi, taqqoslash, maxsus ishlab chiqilgan dasturiy vositalardan foydalangan holda tajribalar o‘tkazish, o‘tkazilgan tajribalar asosida tahlil qilish usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

SM4 va SM4_Mix shifrlash algoritmlari chiziqli kriptotahlil usuli yordamida baholangan va 23-raundli SM4 algoritmi uchun chiziqli tahlilda foydalanish uchun zarur bo‘lgan optimal yaqinlashish tenglamalari ishlab chiqilgan, ushbu tenglamalardan foydalanib, hujumni amalga oshirish uchun $N = 2^{126.4}$ ochiq matn va shifrlangan matn juftliklari zarurligi aniqlangan;

SM4_Mix algoritmi bardoshliligini chiziqli kriptotahlil usuli yordamida baholash jarayonida shakllantirilgan tenglamalardagi noma’lumlar soni SM4 algoritmiga nisbatan 4 martaga ortishi, chiziqlilik darajasi va ularning ehtimolligi farq qilmasligi, ya’ni, 20 raund uchun $2^{-60.5}$ bo‘lishi aniqlangan;

SM4 hamda SM4_Mix shifrlash algoritmlari algebraik kriptotahlil usuli yordamida baholash jarayonida SM4 algoritmining 21 raundi uchun yechish murakkabligi 2^{108} ga teng bo‘lgan 2^{36} ta algebraik tenglamalar, SM4_Mix algoritmining 21 raundi uchun yechish murakkabligi esa 2^{192} ga teng bo‘lgan 2^{64} ta algebraik tenglamalar shakllantirilgan va MixColumns() akslantirishidan foydalanilganda algoritmning algebraik kriptotahlilga bardoshliligi ortishi isbotlangan;

SM4 va SM4_Mix shifrlash algoritmlari tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usuli yordamida baholash jarayonida SM4 algoritmining 4 raundida shifrlash kalitini izlashning murakkabligi 2^{14} ga, SM4_Mix algoritmi uchun 2^{16} ga teng ekanligi aniqlangan;

SM4 algoritmining L va S akslantirishlari uchun optimal amalga oshirish usullari aniqlangan, SM4 va SM4_Mix algoritmlarini apparat ko‘rinishda amalga oshirish uchun kamroq, ya’ni, 26,808 μm² maydonni egallaydigan yuqori o‘tkazuvchanlikka ega hamda 100000 blok ma’lumotni shifrlash uchun 5.234876 sekund hamda shifrni ochish uchun esa 5.482364 sekund sarflanadigan dasturiy ko‘rinishdagi tezkor va samarali usullar taklif qilingan.

Tadqiqotning amaliy natijalari quyidagicha:

SM4 va SM4_Mix simmetrik shifrlash algoritmlarini optimal amalga oshirish uchun dasturiy vositalar ishlab chiqilgan;

SM4 shifrlash algoritmining s-blok jadvali uchun algebraik tenglamalarni shakllantirish uchun dasturiy vosita ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi. Dissertatsiyada olingan natijalarning ishonchliligi unda matematik mulohazalarning qat’iyligi, o‘tkazilgan sonli tadqiqot

natijalari bilan tasdiqlanganligi hamda kriptografik algoritmlarni kriptotahlil usullaridan olingan real hamda tajribaviy tahlillar bilan asoslanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati SM4 simmetrik blokli shifrlash algoritmini chiziqli, algebraik, tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usuli yordamida baholanganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati o‘tkazilgan kriptotahlil usullari natijalaridan va akslantirishlarning kriptografik xarakteristikalaridan zamonaviy shifrlash algoritmlarini kriptotahlil usullari bilan baholashda, yangi shifrlash algoritmlari, yangi akslantirish funksiyalari ishlab chiqishda asos sifatida hamda kriptotahlil usullarini qo‘llanishi o‘rganish jarayonida foydalanish mumkinligi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Kriptotahlil usullari yordamida SM4 algoritmini baholashdan olingan ilmiy natijalar quyidagi yo‘nalishlarda amalda qo‘llandi:

dissertatsiya ishida ishlab chiqilgan SM4 va SM4)Mix shifrlash algoritmlarini amalga oshirishning optimal usullari uchun ishlab chiqilgan dasturiy ta’minotlar “O‘zbektelekom” AK Samarqand shahar telekommunikatsiya bog‘lamasi aloqa va telefoniya tarmog‘ida axborotni uzatish jarayonida qo‘llanilgan (“O‘zbektelekom” AK Samarqand filialining 2024 yil 4 apreldagi 61-03-12/485-sonli ma’lumotnomasi). Ilmiy natijalarning qo‘llanilishi SM4 shifrlash algoritmi uchun taklif qilingan optimal amalga oshirish dasturiy vositasi 1 soniyada 2.21 Mb ochiq ma’lumotni shifrlash va 2.12 Mb shifrlangan ma’lumotni dastlabki holatga o‘girish, SM4_Mix algoritmi uchun taklif qilingan dasturiy amalga oshirish usuli esa 1 soniyada 2.33 Mb ochiq ma’lumotni shifrlash va 2.22 Mb shifrlangan ma’lumotni dastlabki holatga o‘girish imkonini bergan;

dissertatsiya ishida ishlab chiqilgan 23-raundli SM4 algoritmi uchun optimal yaqinlashish tenglamalaridan Wangxin Information Security Service kompaniyasida tijorat kriptografiya ilovalari xavfsizligini baholashda, tarmoqlar va axborot tizimlarida kriptografik ilovalarning muvofiqligi, to‘g‘riligi va samaradorligini baholash bo‘yicha laboratoriya sinovlarida foydalanilgan (Xitoy, Wangxin Information Security Service kompaniyasining 2024 yil 15 martdagi WXSEC20240315001-sonli ma’lumotnomasi). Ilmiy natijalarning qo‘llanilishi SM4 algoritmiga nisbatan chiziqli kriptotahlil hujumini amalga oshirish uchun $2^{126.4}$ ochiq matn va shifrlangan matn juftliklari zarurligi aniqlangan va natijalar SM4 shifrlash algoritmining bardoshligini chiziqli kriptotahlil usuliga baholash jarayonida samarali natijalarga erishish imkonini bergan;

dissertatsiya ishida ishlab chiqilgan SM4 shifrlash algoritmini dasturiy amalga oshirishning optimal usullari, jumladan, SM4 algoritmining L-va S-akslantirishlarini optimal amalga oshirish usullari, SM4 shifrlash algoritmi akslantirishlarini Python dasturlash tilida amalga oshirish usullari, vaqt samaradorligiga erishish imkonini bergan S-boxni bir o‘lchovli jadval sifatida tasvirlash usuli, siklik chapga surish amalini amalga oshirishning aniqlangan samarali usuli, shuningdek, boshqa amalga oshirish usullari bilan solishtirilganda

vaqt bo‘yicha samaradorlikka erishishga imkon bergan shifrlash algoritmini Python dasturlash tilida optimal amalga oshirish natijalari Xitoyning Jining Normal Universitetida Elektron va axborot muhandisligi maktabi tomonidan amalga oshirilgan “SM4 Algoritmi bo‘yicha tadqiqot” nomli jsky2021098 raqamli ilmiy loyihasida blokli shifrlash algoritmlarini baholashda qo‘llanilgan (Xitoy, Jining Normal Universitetining 2024 yil 15 martdagi 20240315-001-sonli ma’lumotnomasi). Ilmiy natijalarning qo‘llanilishi 100 000 blok ma’lumotni shifrlash uchun sarflangan vaqt 5,526601 soniyani, shifrni ochish vaqti esa 5,759675 soniyani tashkil qilgan va taklif qilingan amalga oshirish usullari SM4 shifrlash algoritmining ish faoliyatini yaxshilash imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 3 ta xalqaro va 2 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiya mavzusi bo‘yicha jami 26 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish uchun tavsiya etilgan ilmiy nashrlarida 8 ta, jumladan, Scopus bazasida indekslanadigan nashrlarda 2 ta maqola, xalqaro konferensiyalarda 3 ta, mahalliy konferensiyalarda 2 ta tezis, xorijiy jurnallarda 10 ta maqola chop qilingan, EHM uchun yaratilgan 3 ta dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 101 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, olingan natijalarning ishonchliligi asoslab berilgan, ularning nazariy va amaliy ahamiyati, tadqiqot natijalarini amalda joriy etilish holati, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Feystel tarmog‘iga asoslangan shifrlash algoritmlari. SM4 shifrlash algoritmi va uni kriptotahlil usullari yordamida baholash natijalari”** deb nomlangan birinchi bobida Feystel tarmog‘i asosida ishlab chiqilgan shifrlash algoritmlari, shuningdek, SM4 shifrlash algoritmi, algoritmda foydalanilgan asosiy akslantirishlar, hamda mazkur algoritmni kriptotahlil usullari yordamida baholash natijalari keltirilgan.

Ko‘pgina zamonaviy simmetrik blokli shifrlash algoritmlari Feistel tarmog‘idan foydalanadi, bu tarmoq birinchi bo‘lib Feistel tuzilmasi Horst Feistel va Don Koppersmit tomonidan taklif qilingan IBM kompaniyasining Lucifer (DES algoritmining salafi) shifrlash algoritmida paydo bo‘lgan. Feistel strukturasidan foydalangan holda ishlab chiqilgan shifrlash algoritmlarining ko‘plab turlari mavjud, DES, MISTY1 va SM4 hammasi Feistel tuzilmasidan foydalanadi.

Shuningdek, mazkur tarmoqdan foydalanidan algoritmlar Blowfish, Camellia, CAST-128, FEAL, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, RC5, TEA, Triple DES, Twofish, XTEA, GOST_28147-89, CAST-256, MacGuffin, RC2, RC6 va boshqa algoritmlar hisoblanadi.

SM4 - bu Xitoyning WAPI (Simsiz LAN autentifikatsiya va maxfiylik infratuzilmasi) simsiz LAN xavfsizlik standartida tarkibidagi asosiy blokli shifrlash algoritmdir, bu Xitoy hukumati tomonidan 2006 yilda e'lon qilingan birinchi tijorat kriptografik algoritm hisoblanadi. 2012 yilda u tijorat ma'lumotlari bloklari uchun standart deb e'lon qilindi. 2021-yilda mazkur algoritm xalqaro ISO/IEC standartining bir qismiga aylandi. SM4 o'zining yaratilganidan beri kriptografiya sohasidagi mutaxassislar e'tiborini tortib kelmoqda. Algoritmning xavfsizligi uni doimiy ravishda turli xil tahlil usullari yordamida baholab borishni talab qiladi.

SM4 algoritmining dizayni maqsadi yuqori darajada xavfsiz, samarali va oson amalga oshiriladigan blokli shifrlash sxemasini taqdim etishdan iborat. U 128 bitli kalit va blok o'lchamidan foydalanadi, almashtirish va XOR kabi asosiy operatsiyalarni o'z ichiga olgan 32-raundli iterativ jarayon orqali shifrlash va shifrni ochish jarayonlarini amalga oshiradi. SM4 yuqori xavfsizlikka ega, turli kriptografik xavfsizlik tahlillari va baholashlaridan o'tgan va keng tan olingan va qabul qilingan.

SM4 turli kriptotahlil usullarini qo'llagan holda kriptotahlilchilar tomonidan samarali tarzda kriptotahlil qilingan.

Algoritm ustida olib borilgan kriptotahlillar natijalarining ba'zilari 1-jadvalda keltirilgan.

1-jadval

SM4 algoritmi uchun amalga oshirilgan kriptotahlil natijalari

Kriptotahlil nomi	Hujum amalga oshirilgan raund	Vaqt	Talab qilingan ma'lumot	Talab qilingan xotira
Chiziqli kriptotahlil	24	$2^{122.6}$	$2^{122.6}$	2^{85}
Ko'p o'lchovli chziqli kriptotahlil	23	$2^{122.7}$	$2^{122.6}$	$2^{120.6}$
Differensial kriptotahlil	23	$2^{126.7}$	2^{117}	2^{130}
Matritsali o'lchov kriptotahlil usuli	18	$2^{110.77}$	2^{127}	2^{130}
Takomillashtirilgan differensial kriptotahlil	17	2^{132}	2^{117}	-
Yaxshilangan chiziqli kriptotahlil usuli	14	$2^{120.7}$	$2^{123.5}$	2^{73}
Integral kriptotahlil	14	$2^{96.5}$	2^{32}	-

Dissertatsiyaning **"Kriptotahlil usullaridan foydalangan holda SM4 shifrlash algoritmini baholash"** deb nomlangan ikkinchi bobida SM4 shifrlash algoritmini va uning modifikatsiya qilingan varianti SM4_Mix algoritmini chiziqli,

algebraik, tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usullariga baholash natijalari keltirilgan.

Chiziqli kriptotahlil simmetrik kalit kriptografik primitivlarini o‘rganishning eng muhim usuli sifatida ajralib turadi. Bu usul birinchi navbatda ochiq matn, shifrlangan matn va kalit o‘rtasida chiziqli yaqinliklarni o‘rnatishga qaratilgan. Chiziqli kriptotahlil ostida shifr tasodifiy bo‘lmagan almashtirish xatti-harakatini ko‘rsatsa, qo‘shimcha raundlarni kiritish orqali farqlovchini yaratish yoki hatto kalitni tiklash hujumini boshlash mumkin bo‘ladi. Ushbu jarayon qo‘shilgan turlarning pastki bo‘limlari haqida bilimli taxminlarni amalga oshirishni, shifrlangan matnlarning shifrini ochishni va/yoki diskriminator uchlaridagi oraliq holatni hisoblash uchun ushbu bo‘limlar yordamida ochiq matnlarni shifrlashni o‘z ichiga oladi. Agar kichik bo‘limlar to‘g‘ri taxmin qilinmasa hujum muvaffaqiyatsiz bo‘ladi. Chiziqli kriptotahlil turli xil shifrlarni tahlil qilishda qo‘llanilgan.

Oldingi barcha SM4 algoritmiga nisbatan amalga oshirilgan hujumlarida raundlar soni bo‘yicha samaradorlikka kelsak, kalitlarni tiklashning eng samarali usullari chiziqli kriptotahlil va differensial kriptotahlildir. Ikkala yondashuv ham 19 raundgacha muvaqqiyatli farqlovchilar orqali amalga oshirilgan. Mazkur tadqiqot ishining asosiy maqsadi SM4 ga hujumlarni kuchaytirish, samaraliroq farqlovchilarni izlashdir. Shunday qilib, asosiy e’tibor SM4 uchun chiziqli yaqinlashishni o‘rganishga qaratilgan.

Eng samarali oldingi chiziqli hujumlar 19-raundli chiziqli yaqinlashishga qaratilgan. Bunga javoban, mazkur ishda SM4 algoritmida oz sonli raundlarda iterativ chiziqli yaqinlashish uchun maxsus ishlab chiqilgan yangi qidiruv algoritmi taqdim etildi. Bu S-boxning qisman chiziqli yaqinlashish jadvalini muntazam ravishda kengaytirishni o‘z ichiga oladi. Dastlab, SM4 uchun bir yoki ikki raundli iterativ chiziqli yaqinlashuvlar mavjud emasligi ko‘rsatilgan. Keyinchalik, 3-raund SM4 ning iterativ chiziqli yaqinlashuvlari uchun ma’lum xususiyatlar olinadi. Ushbu xususiyatlardan foydalangan holda, bizning qidiruv algoritmimiz $2^{-57,3}$ ehtimollikka ega bo‘lgan 19 raundli chiziqli yaqinlashuvni va $2^{-60,5}$ ehtimollik bilan 20-raundli chiziqli yaqinlashuvni olish uchun qo‘llaniladi. Bizning aniqlangan chiziqli yaqinlashuvlar oldingilari bilan taqqoslash 2-jadvalda keltirilgan. Shunisi e'tiborga loyiqki, mazkur ishda olingan chiziqli yaqinlashishlar bugungi kungacha eng samarali ekanligini ko‘rish mumkin.

2-jadval.

SM4 uchun chiziqli approksimatsiyalar

Manba	Ehtimolli	Raundlar
[29]	$2^{-62.27}$	19
[14]	2^{-58}	19
[14]	2^{-61}	20
Mazkur ish	$2^{-57.3}$	19
Mazkur ish	$2^{-60.5}$	20

Eng samarali oldingi hujumlar SM4 uchun 23 raundgacha samaradorlikni ko‘rsatdi. SM4 uchun aniqlangan 20-raundli chiziqli yondashuvimizdan foydalanib,

biz SM4 uchun raundlar soniga ko‘ra hozirda eng kuchli hujum bo‘lgan 24-raundli SM4-ga qaratilgan asosiy kalitni tiklash hujumini joriy qilish mumkin. Bundan tashqari, biz 23-raundli SM4-ga hujumni boshlash uchun yangi o‘rnatilgan 19-raundli chiziqli yondashuvdan foydalanish va shu bilan 23-raundli SM4-da oldingi eng yaxshi chiziqli hujumning samaradorligini oshirish mumkin. Bu hujumlar va SM4 uchun avval o‘tkazilgan hujumlar haqida umumiy ma’lumot 3-jadvalda keltirilgan.

Teorema 1. 19-davrali chiziqli yaqinlashuvni qurish uchun ketma-ket ikkita faol raundda T funktsiyalarining kirish maskalari bir xil bo‘lishi kerak.

3-jadval.

SM4 algoritmiga nisbatan amalga oshirilgan kriptotahlil hujumlari

Kriptotahlil usuli	Raundlar soni	Vaqt (T)	Ma’lumot (D)	Manba
To‘rtburchak	16	2^{116}	2^{125}	[23][25]
To‘rtburchak	14	$2^{87.69}$	$2^{107.89}$	[17][18]
To‘rtburchak	18	$2^{112.83}$	2^{124}	[10]
Integral	13	2^{114}	2^{16}	[6]
Mumkin bo‘lmagan differensial	16	$2^{96.07}$	$2^{117.06}$	[18]
Boomerang	18	$2^{116.83}$	2^{120}	[10]
Differensial	21	$2^{126.6}$	2^{118}	[26]
Differensial	23	$2^{126.7}$	2^{118}	[13]
Differensial	22	$2^{125.71}$	2^{118}	[10]
Differensial	22	$2^{112.3}$	2^{117}	[12]
Chiziqli	22	2^{117}	$2^{118.4}$	[11]
Chiziqli	22	$2^{109.86}$	2^{117}	[10]
Chiziqli	23	2^{122}	$2^{126.54}$	[24]
Ko‘p chiziqli hujum	22	$2^{119.75}$	2^{112}	[27]
Ko‘p o‘lchovli chiziqli	23	$2^{127.4}$	$2^{126.6}$	[14]
Ko‘p o‘lchovli chiziqli	23	$2^{122.7}$	$2^{122.6}$	[24]
Chiziqli	23	$2^{121.7}$	$2^{126.4}$	Mazkur ish
Ko‘p o‘lchovli chiziqli	23	$2^{122.5}$	$2^{122.3}$	Mazkur ish

Isbot. Agar Γ_{in}^{i} and Γ_{in}^{i} $(i = 1,\cdots,6)$ naqshli oltita raundli chiziqli yaqinlashishda T funksiyalarining kirish va chiqish maskalarini ifodalasa. Bundan esa, $\Gamma_{in}^{3}\oplus\Gamma_{out}^{1}\oplus\Gamma_{in}^{2} = \Gamma_{in}^{4}\oplus\Gamma_{out}^{5}, \Gamma_{in}^{4}\oplus\Gamma_{out}^{6}\oplus\Gamma_{in}^{5} = \Gamma_{in}^{3}\oplus\Gamma_{out}^{2}$ bo‘ladi. $j = 1,2,5,6$

uchun $\Gamma_{in}^{j} = \Gamma_{out}^{j} = 0$ o‘rinli ekanligidan $\Gamma_{in}^{3} = \Gamma_{in}^{4}$ kelib chiqadi. Teorema 1 isbot qilindi.

SM4 algoritmida ishlatiladigan siklik chapga siljish akslantirishi o‘rniga AES algoritmida foydalanilgan MixColumns() chiziqli akslantirishi qo‘llanilsa mazkur kriptotahlil natijalari qanday bo‘lishi mumkinligi ham ko‘rib chiqildi.

MixColumns ko‘rinishida holat ustuni elementlari ushbu polinom algoritmida berilgan uchinchi darajadan katta bo‘lmagan ko‘phadning koeffitsientlari sifatida ifodalanadi: g(x) = {03}x3 +{01}x2 +{01}x+{02}. Ko‘paytirish natijalari x^4+1 ko‘phadga bo‘lib qoldiqni olish orqali ko‘phad ko‘rinishda hisoblanadi.

SM4 shifrlash algoritmida ishlatiladigan siklik chapga siljish akslantirishi o‘rniga MixColumns() akslantirishida foydalanish har bir bit o‘rniga 4 bit hosil bo‘lishiga olib kelishini ko‘rishimiz mumkin. Siklik surish amalida esa bu 1 bitga teng. Bundan xulosa qilish mumkinki, MixColumns() akslantirishidan foydalanilganda u chiziqli kriptotahlil jarayonida faqat tenglamalardagi noma’lumlar soniga ta’sir qiladi, chiziqlilik darajasi va ularning ehtimoliga ta’sir qilmaydi.

SM4 shifrini algebraik tahlilini modellashtirishda tenglamalar tizimini qurish uchun ishlatiladigan asosiy transformatsiya S-boxlar ichida chiziqli bo‘lmagan almashtirish ekanligini ta’kidlash muhimdir. Kirish va chiqish bloklari bitlari kompozitsiyalarining umumiy sonini t sifatida ifodalanadi. Binobarin, kamida $t - 2^s$ chiziqli mustaqil tenglamalar mavjud bo‘lib, ular 1 ehtimollik bilan to‘g‘ri hisoblanadi.

Misol tariqasida, $s \times s$ -bitli S-box uchun mantiqiy chiziqli bo‘lmagan tenglamalar quyidagicha aniqlanadi (1- tenglama):

$$\sum_{i,j,k=0}^{s-1} \alpha x_i y_j y_k + \sum_{i,j,k=0}^{s-1} \beta x_i x_j y_k + \sum_{i,j=0}^{s-1} \gamma x_i y_j + \sum_{i,j=0}^{s-1} \delta y_i y_j + \sum_{i=0}^{3} \lambda x_i + \sum_{i=0}^{3} \omega y_i + \eta = 0 \quad \textbf{(1)}$$

bu yerda $\alpha, \beta, \gamma, \delta, \lambda, \omega, \eta$ – ikkilik koeffisiyentlar;

x_i va y_i - mos ravishda S-boxning kirish va chiqish vektorlarining i-bitiga kirish va chiqish bitlari;

s kirish va chiqish vektorlarining uzunligini ifodalaydi.

Tenglama (2) 3 yoki undan kam darajali mumkin bo‘lgan tenglamalar sonini hisoblash uchun ishlatiladi:

$$t = \binom{2s}{3} + \binom{2s}{2} + 2s + 1 \quad \textbf{(2)}$$

8 × 8 bitli S-qutili SM4 shifrida t bilan belgilangan monomiallarning umumiy soni quyidagicha olinadi:

$$t = \binom{16}{3} + \binom{16}{2} + 16 + 1 = 697 \quad \textbf{(3)}$$

Binobarin, $r \geq t - 2^8 = 441$ chiziqli mustaqil 3-darajali tenglamalarni aniqlash mumkin. SM4 chiziqsiz almashtirish akslantirishi uchun 3-darajali mantiqiy tenglamalar tizimi 1-rasmda ko‘rsatilgan kabi tenglamalarni o‘z ichiga oladi.

SM4 shifrining S-box akslantirishi 441 chiziqli mustaqil tenglamalar orqali ifodalanadi, ularning umumiy soni 697 dan oshmaydi. SM4 shifrlash algoritmining bir bosqichi, yagona chiziqli bo‘lmagan akslantirishi va boshqa chiziqli akslantirishlar natijasida hosil bo‘ladi. Bit almashinuvida 64 ta noma’lum (raund kaliti rk va S-boxlardan chiqish vektori) bilan 1764 3-darajali chiziqli mustaqil tenglamalar tizimi sifatida tasvirlanishi mumkin. SM4 ning to‘liq versiyasi uchun (32 tur) 2048 noma’lum bo‘lgan 56448 kubik tenglamalar to‘plami tuzilgan (32 rk_i va 32 S-box chiqish vektori).

x3y0+x2y7+x2y1+x1y7+x1y3+x1y2+x1y1+x1y0+y6+y5+y4+y3+y2+y1+y7+y3+y1+y0+x7x6x5+x7x6x3+x7x6x2+x7x6x1+x7x6+x7x5x4+x7x5x3+x7x5x2+x7x5+x7x4x1+x7x4x0+x7x4+x7x3x0+x7x2x1+x7x2+x7x1+x7x0+x7+x6x5x4+x6x5x3+x6x5x2+x6x5+x6x4x2+x6x4x1+x6x4+x6x1x0+x6x1+x6x0+x6+x5x4x0+x5x3+x5x2x1+x5x2x0+x5x2+x5x1+x5x0+x5+x4x3x2+x4x3+x4x1x0+x3x2x0+x3x1x0+x2x1x0+x2+x1x0+x0=0

x3y2+x3y1+x2y7+x2y6+x2y5+x2y4+x2y3+x2y1+x2y0+x1y5+x1y4+x1y2+y6+y5+y1+y0+x7x6x4+x7x5x4+x7x5x3+x7x4x1+x7x4x0+x7x3+x7x2x0+x7x1x0+x7x1+x7+x6x5x4+x6x5x2+x6x5x0+x6x5+x6x4x3+x6x4x2+x6x4x0+x6x3x0+x6x3+x6x2x1+x6x1x0+x6x1+x6+x5x4x3+x5x4x2+x5x4x1+x5x4x0+x5x3x2+x5x3+x5x2x0+x5x2+x4x3x0+x4x2x0+x4x1x0+x4x1+x4x0+x4=0

x3y3+x3y1+x2y3+x2y2+x1y7+x1y6+x1y4+x1y3+x1y0+y5+y7+y5+y4+y3+y2+y1+y0+x7x6x5+x7x6x3+x7x6x2+x7x6x1+x7x6x0+x7x6+x7x5x4+x7x5x3+x7x5x2+x7x5x1+x7x5x0+x7x5+x7x4x3+x7x4x2+x7x4+x7x3x0+x7x3+x7x2x0+x7x2+x7x1x0+x7x1+x7x0+x6x5x0+x6x5+x6x4x3+x6x4x1+x6x4+x6x3x2+x6x3x0+x6x2x1+x6x2x0+x6x1+x6x0+x6+x5x4x3+x5x4x2+x5x4x1+x5x4x0+x5x3x2+x5x3x0+x5x2x0+x5x2+x5x1x0+x5x1+x5+x4x2+x4x1x0+x4+x3x2x1+x3x1x0+x3x1+x2x1x0+x1x0+x1=0

…..

1-rasm. SM4 algoritmi S-boxi uchun 3-darajali tenglamalarning ko‘rinishi

x4y0+x3y6+x3y2+x3y0+x2y6+x2y4+x2y3+x2y0+x1y7+x1y5+x1y4+x1y3+x1y0+y7+y5+y4+y3+y2+y0+y6+y5+x7x6+x7x5+x7x4+x7x3+x7x2+x7x1+x6x4+x6x2+x6x1+x5x4+x5x3+x5x2+x5x1+x4x2+x4x0+x4+x3x2+x3x1+x3x0+x2x0+x2=0

x4y1+x3y4+x3y2+x3y1+x2y5+x2y4+x2y3+x2y1+x2y0+x1y7+x1y5+x1y2+x1y1+y6+y4+y3+y1+y6+y3+x7x6+x7x5+x7x2+x7x1+x6x5+x6x2+x5x4+x5+x4x0+x4+x3x1+x3x0+x2x1+x2x0+x1x0+x0=0

x4y2+x3y5+x3y4+x3y2+x3y0+x2y7+x2y6+x2y5+x2y4+x2y3+x2y2+x2y1+x2y0+x1y4+x1y3+x1y2+x1y0+y4+y3+y2+x7x4+x7x2+x7x1+x7x0+x7+x6x5+x6x4+x6x3+x6x1+x6+x5x4+x5x0+x4x2+x2x0+x2+x1x0=0

x4y4+x4y3+x3y1+x2y7+x2y4+x2y2+x2y1+x1y6+x1y5+x1y3+x1y1+x1y0+y7+y5+y3+y2+y6+y5+y4+y2+y0+x7x5+x7x4+x7x2+x6x5+x6x4+x6x3+x6x0+x5x3+x5x1+x5+x4x0+x3x1+x2x0=0

x4y5+x4y3+x3y7+x3y1+x3y0+x2y7+x2y5+x2y4+x2y3+x2y1+x2y0+x1y7+x1y5+x1y4+x1y3+x1y2+x1y0+y7+y6+y5+y4+y2+y0+y5+y3+y2+y1+x7x4+x7x0+x7+x6x5+x6x3+x6x1+x6x0+x6+x5x4+x5x2+x5x1+x5+x4x3+x4x1+x4x0+x4+x3x1+x3x0+x3+x2+x1=0

x4y6+x3y6+x3y5+x3y4+x3y2+x3y1+x2y7+x2y4+x2y2+x2y1+x2y0+x1y6+x1y5+x1y4+x1y3+x1y1+y6+y2+y1+y7+y3+y1+x7x5+x7x4+x7x2+x7x1+x7x0+x6x4+x6x0+x6+x5+x4x1+x4x0+x3x2+x3x1+x3x0+x2x1+x2+x1x0+x0=0

……..

2-rasm. SM4 algoritmi S-boxi uchun 2-darajali tenglamalarning ko‘rinishi

SM4 shifrlash algoritmining S-box almashtirish jadvali uchun 2-darajali tenglamalar tizimini shakllantirish ham mumkin. SM4 almashtirish bloki uchun 2-darajali mantiqiy tenglamalar 2-rasmda ko‘rsatilgandek tenglamalarni o‘z ichiga oladi.

Teorema 2. Algoritmda foydalanilgan chapga siljitish akslantirishi o‘rniga MixColumns() akslantirishi qo‘llanilganda algoritmning algebraik kriptoanalizga bardoshliligi ortadi.

Isbot. SM4 shifrlash algoritmi uchun chiziqli bo‘lmagan tenglamalar soni, noma’lumlar soni va yechishning murakkabligi haqidagi ma’lumotlar quyidagi 4-jadvalda keltirilgan.

Ushbu jadvaldan SM4 shifrlash algoritmi 22-turdan so‘ng algebraik kriptotahlil usuliga bardoshli ekanligini va MixColumns() akslantirishi qo‘llanilganda algoritmning algebraik kriptoanalizga bardoshliligi ortishini ko‘rish mumkin. Teorema 2 isbot qilindi.

4-jadval

SM4 algoritmining raundlari uchun shakllantirilgan algebraik tenglamalarning xususiyatlari

Raundlar	**Chiziqli bog‘liq bo‘lmagan tenglamalar**	**Noma’lumlar soni**	**Yechish murakkabligi**
1	39	2^{6}	2^{18}
5	2535	2^{12}	2^{36}
9	5031	2^{18}	2^{54}
13	7527	2^{24}	2^{72}
17	10023	2^{30}	2^{90}
21	12519	2^{36}	2^{108}
25	15015	2^{42}	2^{120}

Algebraik kriptotahlilni algoritmning SM4_Mix varianti uchun ham amalga oshirilishi mumkin. Chiziqli kriptotahlil jarayonida ta’kidlanganidek, MixColumns() akslantirishi sistemadagi noma’lumlar soniga ta’sir qiladi. Ya’ni, algebraik tahlilda s_box chiqishidagi bitlar uchun tuzilgan tenglamalarning aksariyati MixColumns() akslantirishidan olingan natijani ifodalashda ishtirok etadi. 5-jadvalda algoritmning SM4_Mix varianti uchun raundlarni ifodalovchi tenglamalardagi o‘zgaruvchilar soni va ularni yechish murakkabligi keltirilgan.

5-jadval

SM4 algoritmining raundlari uchun shakllantirilgan algebraik tenglamalarning xususiyatlari

Raundlar	**Chiziqli bog‘liq bo‘lmagan tenglamalar**	**Noma’lumlar soni**	**Yechish murakkabligi**
1	39	2^{6+4}	2^{30}
5	2535	2^{20+4}	2^{72}
9	5031	2^{30+4}	2^{112}
13	7527	2^{40+4}	2^{132}
17	10023	2^{50+4}	2^{162}
21	12519	2^{60+4}	2^{192}
25	15015	2^{70+4}	2^{222}

Ushbu jadvaldan xulosa qilish mumkinki, agar SM4 algoritmida qo‘llaniladigan siklik surish akslantirishi o‘rniga MixColumns() akslantirishi

ishlatilsa, algoritmning algebraik kriptotahlilga bardoshliligi ortadi. Masalan, SM4 algoritmining 21 ta raundini ifodalovchi tenglamalardagi noma'lumlar soni 2^{36} ta, yechishning murakkabligi esa 2^{108} ta, SM4_Mix da noma'lumlar soni 2^{64} ta, yechimning murakkabligi esa 2^{192} ta. Ikkala holatda ham tuziladigan tenglamalar soni farq qilmaydi.

Shunigdek, SM4 shifrlash algoritmini tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usuliga ham baholash amalga oshirildi. Agar hujum muvaqqiyatli amalga oshirilsa, ikki yoki to‘rt raundning tahlili orqali SM4 ning butun 128 bitli kaliti to‘liq qayta tiklanishi mumkin. Ushbu yondashuv an'anaviy tanlangan ochiq matnli hujumlarga nisbatan bir qancha afzalliklarga ega.

SM4 ga tanlangan ochiq matnli hujum (L) chiziqli akslantirishidan so‘ng chiqish resursini o‘zgartirish uchun belgilangan cheklovlarga ega bo‘lgan aniq matnlarni tanlashni o‘z ichiga oladi. Keyinchalik, X_{i+4} raund chiqishi hujum uchun nishon sifatida tanlanadi ($X_{i+4} = X_i \oplus res$, bu erda X_i tasodifiy qiymat ma'lum va res - belgilangan noma'lum qiymat). Kuchga asoslangan tahlil qilish orqali belgilangan qiymat res aniqlanadi, bu raund kalitini olib tashlashga imkon beradi. SM4 uchun umumiy kalitni tiklash birinchi to‘rtta raundda tanlangan ochiq matnli hujumni ketma-ket bajarishni o‘z ichiga oladi.

Ilgari tanlangan ochiq matnli hujumdan farqli o‘laroq, ushbu ishda taqdim etilgan integratsiyalangan raundlar sonini qisqartirish hujumi hujum uchun zarur bo‘lgan raundlar soni, hujum nuqtalarini tanlash va izlarni yig‘ish chastotasi bo‘yicha aniq afzalliklarni namoyish etadi.

6-jadvalda ko‘rsatilganidek, mazkur qo‘shma hujum hujum raundlari sonini yarmiga qisqartiradi, bu faqat ikkita iz to‘plamini talab qiladi, bu ochiq matnlarning ko‘proq tanlanishini o‘z ichiga olgan oldingi hujumlarga nisbatan sezilarli yaxshilanish hisoblanadi va hujumning umumiy samaradorligini oshiradi. Shuningdek, oldingi chiziqli XOR yoki L akslantirishi va raund chiqishi o‘rniga hujum nuqtasi sifatida S-boxning chiqishiga e'tibor qaratilsa hujumning muvaffaqiyat darajasi samarali ravishda oshadi. Bundan tashqari, mazkur hujumdagi dastlabki to‘rt raundning kalitlarini tiklash uchun zarur bo‘lgan izlarning umumiy soni (4 × N, bu erda N bitta muvaffaqiyatli hujum uchun izlar sonini bildiradi) tegishli talabdan (16 × N) sezilarli darajada past). Izlarning umumiy soni ham 4 × N bo‘lsa-da, ushbu qo‘shma hujum bunga faqat ikkita raund va ikkita iz to‘plami bilan erishadi, bu ham izlarni to‘plash vaqtini, ham umumiy hujum vaqtini qisqartiradi. Va nihoyat, kalit qidiruv maydonining murakkabligi avvalgi tanlangan ochiq matnli hujumlarga nisbatan kichikroq.

SM4_Mix varianti uchun ushbu kriptotahlilni o‘tkazishda MixColumns() akslantirishidagi differensial farqlar darajasi SM4 algoritmiga nisbatan 4 barobar, murakkabligi ham 4 baravar yuqori ekanligi kuzatiladi.

6-jadval.

SM4 va SM4_Mix algoritmlariga o‘tkazilgan hujumlarning qiyosiy tahlili

Manba	Kuchga asoslanga hujumning oraliq qiymati	Kuzatuv olib boriladigan izlar soni	Izlarning umumiy soni	Kalitni aniqlashning murakkabligi
[62]	1, 2, 3 va 4 raundlardagi L akslantirish	16	$16 \times N$	$4 \times 4 \times 2^8$
[63]	1, 2, 3 va 4 raundlardan chiqish qiymati	4	$4 \times N$	$4 \times 4 \times 2^8$
[64]	1, 2, 3 va 4 raundlardan chiqish qiymati	16	$16 \times N$	$4 \times 4 \times 2^8$
[65]	1, 2, 3 va 4 raundlardan chiqish qiymati	16	$16 \times N$	$4 \times 4 \times 2^8$
[79]	2- va 4- raundlarning S-box akslantirishidan chiqishi	2	$4 \times N$	$(4 \times 2^4 \times 2^8) \times 2$
SM4	2- va 4- raundlarning S-box akslantirishidan chiqishi	2	$4 \times N$	$(4 \times 2^4 \times 2^8)$
SM4_Mix	2- va 4- raundlarning S-box akslantirishidan chiqishi	2	$16 \times N$	$(16 \times 2^4 \times 2^8)$

Dissertatsiyaning **“SM4 shifrlash algoritmini dasturiy va aprratda optimal amalga oshirish usullarini ishlab chiqish”** deb nomlangan uchinchi bobida SM4 shifrlash algoritmini va uning modifikatsiya qilingan varianti SM4_Mix algoritmini dasturiy hamda apparatda amalga oshirish usullari o‘rganilgan va amalga oshirishning optimal usullari taklif qilingan.

Python dasturlash tilida almashtirish jadvallari (S-box) uchta usulda ifodalanishi mumkin. Bular lug‘at (dictionary) ko‘rinishi (Sbox_dict), 1 (Sbox_Table1) va 2 (Sbox_Table1) o‘lchovli massivlar (dimensional arrays) shaklida. Ushbu ifodalash usullariga ko‘ra, ushbu jadvallarga murojaat qilish usullari ham farqlanadi.

O‘zgartirish jadvalining ko‘rinish shakliga ko‘ra, ularga murojaat qilish uchun funktsiyalar quyidagilardir:

(1) Lug‘at ko‘rinishida ifodalangan holat uchun mos murojaat funktsiyasi (def tau_dict(input: int) -> int);

(2) 1-o‘lchovli massiv sifatida ifodalangan holat uchun mos murojaat funksiyasi (def tau1(input: int) -> int);

(3) 2-o‘lchovli massiv sifatida ifodalangan holat uchun mos murojaat funksiyasi (def tau2(a)).

Yuqoridagi murojaat funksiyalaridan foydalangan holda 10 000 000 tasodifiy 32-bit qiymatlarni almashtirish jadvaliga murojaat qilish uchun sarflangan vaqt qiymatlari quyidagi 7-jadvalda ko‘rsatilgan.

7-jadval.

10 000 000 tasodifiy 32 bitli qiymatlarni almashtirish jadvaliga murojaat qilish uchun sarflangan vaqt qiymatlari

No.	S_box ni ifodalash usuli	Murojaat funksiyasi	Vaqt sarfi (sec)
1.	dictionary view (Sbox_dict)	def tau_dict(input: int) -> int	16.1635637283325
2.	1 dimensional arrays (Sbox_Table1)	def tau1(input: int) -> int	12.3912270069122
3.	2 dimensional arrays (Sbox_Table2)	def tau2(a)	14.3787536621093

Chapga siklik siljish jarayoni Python dasturlash tilida ham turli yo‘llar bilan ifodalanishi mumkin. Ushbu usullar va SM4_Mix algoritmining MixColumns() akslantirishining Pythonda ifodalanishlari quyida keltirilgan.

(1) chapga siklik chapga siljitish akslantirishini 1-usuli;

```
def left_shift_1(a: int, n: int) -> int:
                for i in range(n):
                  a <<= 1
              if a // 0x100000000 == 1:
                a %= 0x100000000
                    a += 1
                    return a
```

(2) chapga siklik chapga siljitish akslantirishini 2-usuli;

```
        def left_shift_2(a:int, n:int):
              size=32
              n =n% 32
              return (a << n) | (a >> (size - n)) &0xffffffff
```

(3) chapga siklik chapga siljitish akslantirishini 3-usuli;

```
def left_shift_2(a:int, n:int):
         size=32
         n =n% 32
      return (a << n) ^ (a >> (size - n)) &0xffffffff
```

(4) MixColumns() Lut_table bilan;

```
         import time
         def mixColumns(input):
        a = input // 0x01000000
        b = (input & 0x00ff0000) >> 16
```

```
c = (input & 0x0000ff00) >> 8
d = input % 0x100
a1=mul2[a] ^ mul3[b] ^ c ^ d
b1=a ^ mul2[b] ^ mul3[c] ^ d
c1=a ^ b ^ mul2[c] ^ mul3[d]
d1=mul3[a] ^ b ^ c ^ mul2[d]
```

(5) MixColumns();

```
def gmul(a, b):
if b == 1:
return a
tmp = (a << 1) & 0xff
if b == 2:
return tmp if a < 128 else tmp ^ 0x1b
if b == 3:
return gmul(a, 2) ^ a
t1=time.time()
for i in range(100000000):
mixColumns(0xA3B1BAC6)
t2=time.time()
print(t2-t1)
```

8-jadvalda 100 000 000 ta tasodifiy butun sonlarda chapga siljitish operatsiyasini bajarish uchun yuqoridagi uchta variant hamda MixColumns akslantirishi uchun keltirilgan ikkita variant uchun olingan vaqt sarfi ko‘rsatilgan.

8-jadval.

Chapga siklik siljitish Mixcolumns() akslantirishlarini 100 000 000 asodifiy 32 bitli qiymat uchun amalga oshirishning vaqt sarfi

No.	Ifodalash usuli	Vaqt sarfi (sec)
1.	1-usul	403.48764538764954
2.	2-usul	142.70483493804932
3.	3-usul	142.435124874115
4.	4-usul (MixColumns())	687.4968481063843
5.	5-usul (MixColumns()Lut_table bilan)	134.1191828250885

MixColumns() Lut_table bilan (5-usul) qatori oldindan hisoblangan jadval yordamida MixColumns natijalarini hisoblash uchun sarflangan vaqtni tavsiflaydi.

8-jadvalda Python dasturlash tilida chapga siljitish akslantirishini 3-usulda bajarish maqsadga muvofiqdir. Eng ko‘p vaqt 1-usulga sarflangan. 3-usulda or va xor amallari tufayli 2-usulga nisbatan bir oz kamroq vaqt sarflangan. Shuningdek, oldindan hisoblangan jadvallardan foydalanilganda MixColumns() ko‘rsatish siklik chapga siljitishga qaraganda tezroq ekanligini ko‘rish mumkin.

Ushbu dastur kodidan foydalangan holda 100 000 blokli ochiq matnni shifrlash va shifrini ochish uchun sarflangan vaqt boshqa tadqiqotchilar taklif qilgan amalga oshirish usullari bilan solishtirildi. 9-jadvalda taqqoslash natijalari ko‘rsatilgan.

9-jadvaldagi natijalardan shuni ko‘rishimiz mumkinki, ushbu ishda taklif qilingan amalga oshirish usuli boshqa tavsiya etilgan amalga oshirish usullariga nisbatan vaqt bo‘yicha samarali ko‘rsatkichga ega.

9-jadval.

100 000 blokni shifrlash va shifrini ochish uchun sarflanadigan vaqt

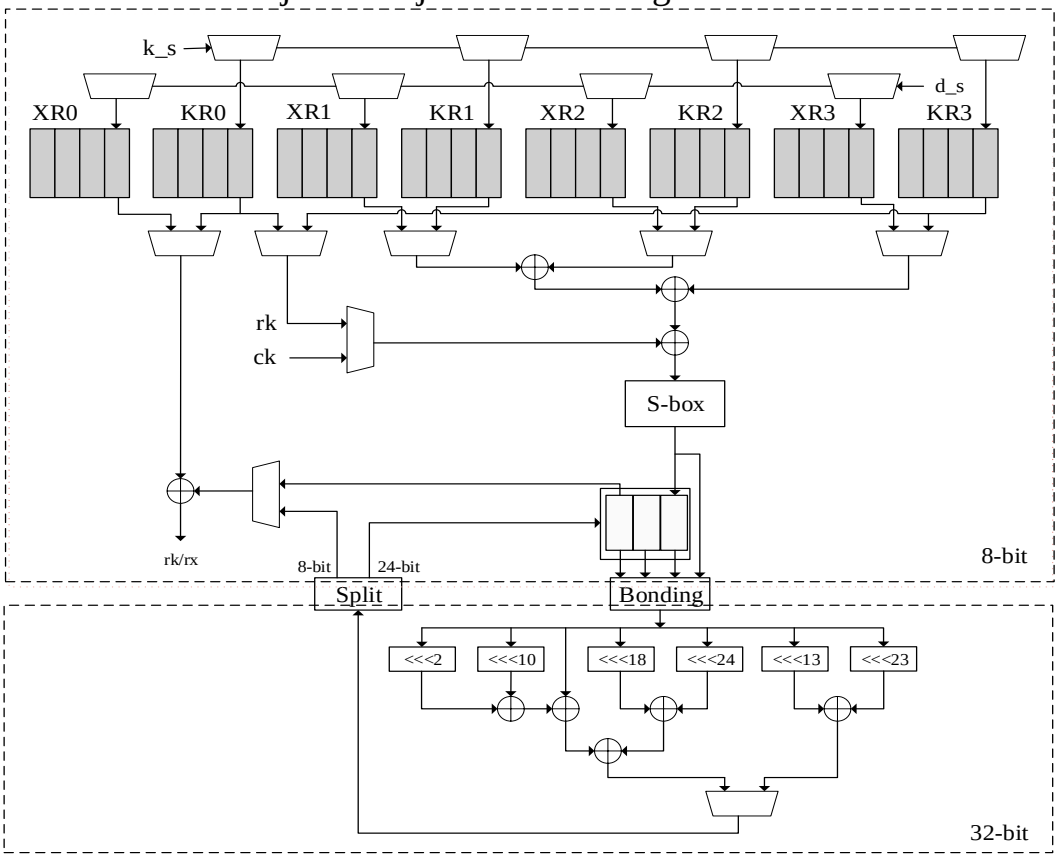
No.	Amalga oshirish usuli	Vaqt sarfi (sec) (SM4 va SM4_Mix)	
		Shifrlash	Shifrni ochish
1.	Miao X. et al.	36.23312	36.06769
2.	https://github.com/CCWUCMCTS/SM4/blob/main/SM4.py	9.26895	10.14109
3.	https://github.com/windard/sm4/blob/master/Python/sm4.py	6.723578	6.760374
4.	Mazkur ish (SM4)	5.526601	5.759675
5.	SM4_Mix	18.53468	18.74289
6.	SM4_Mix (Lut_table)	5.234876	5.482364

Ushbu ishda shuningdek ultra arzon SM4 (ULSM4_2) deb nomlangan SM4 ning yangi apparat tatbiqi taqdim etildi. UCSM4 ga o‘xshab, ULSM4 ning iteratsiya tuzilishi jarayon birligi sifatida 8 bitli ma’lumotlar kengligini qabul qiladi va kalitlarni kengaytirish va shifrlash hisoblarini osonlashtiradi. Asosiy yangilik SM4 ning 8-bitli iteratsiya strukturasidagi tenglamalar orqali tezkor kalitlarni kengaytirish va doimiy kalitlarni dinamik ishlab chiqarishdan foydalanish hisoblanadi, bu esa maydonning sezilarli qisqarishiga olib keladi. ULSM4_2 so‘nggi ish UCSM4 o‘rtasidagi mantiqiy sintez natijalariga asoslangan taqqoslash shuni ko‘rsatadiki, ULSM4 SMIC18 texnologiyasida atigi 2,51 K gate larni talab qiladi, bu UCSM4 bilan solishtirganda 18,0% ga samaradorlikni anglatadi. Hududni minimallashtirishning ushbu usullari ularning samaradorligini ko‘rsatadi, ULSM4 ni resurslar cheklangan qurilmalar uchun ko‘proq mos tanlov sifatida taklif qilish mumkin.

SM4 arxitekturasi 8-bitli, chiziqli almashtirishdan tashqari, chapga 32-bitli aylana siljishini o‘z ichiga oladi va bayt operatsiyalariga bo‘lib bo‘lmaydi. XR va KR registrlari har bir takt siklida 8 bitni chapga siljitib, siljish registrlari vazifasini bajaradi. Faqat eng o‘ng bayt d_s yoki k_s tomonidan boshqariladigan 8 bitli multipleksor orqali yangilanadi va 8 bitli XOR operatsiyalari uchun tanlanadi. BR registri chapga siljish registrlari bo‘lib xizmat qiladi, S-Box chiqishini raundlarning dastlabki uchta siklida saqlaydi va oxirgi siklda chiziqli almashtirish chiqishining pastki 24 bitini saqlash uchun mo‘ljallangan. Chiqish interfeysi 8 bitli va natijalarni qaytarish uchun to‘rtta sikl kerak bo‘ladi. Shifrlash uchun raund kaliti rk KR3 registridan, shifrni ochish uchun esa KR0 registridan olinadi.

UCSM4_2 kalitni kengaytirish va shifrlash uchun umumiy yagona S-Box bilan 8 bitli iteratsiya tuzilishiga ega. Raund kalitlari oldindan hisoblab chiqiladi va xotirada saqlanadi va doimiy kalitlar qidiruv jadvali (LUT) yordamida amalga oshiriladi. OTFSM4 deb nomlangan qo‘shimcha dizayn UCSM4 asosida amalga

oshirilgan bo‘lib, tezkor kalitni kengaytirishni qo‘llaydi. OTFSM4 da doimiy kalitlar LUT yordamida ham amalga oshiriladi, lekin ular qayta rejalashtirilmaydi. Shuning uchun, asosiy kengaytirish mexanizmi UCSM4_2 va OTFSM4 o‘rtasidagi asosiy farqdir. Solishtirish natijalari 10-jadvalda keltirilgan.



3-rasm. ULSM4_2 amalga oshirish usulining iteratsiya tuzilishi

10-jadval.

SMIC18 mantiqiy qurilma va 185 MGts uchun solishtirish natijalari

Amalga oshirish usuli	Maydon/ μm²			Gate lar soni
	Combinatsiyalangan	Combinatsiyalanmagan	Umumiy	
UCSM4 [98]	19,772	10,797	30,569	3060
OTFSM4 [102]	11,794	13,513	25,308	2530
ULSM4 [102]	11,557	13,496	25,053	2510
OTFSM4_2 [mazkur ish]	11,744	13,484	25,228	2490
ULSM4_2 [mazkur ish]	11,512	13,444	24,956	2470
SM4_Mix	15,494	16,744	32,238	2840
SM4_Mix (Lut_table bilan)	12,356	14,452	26,808	2560

Shuningdek, ULSM4_2, SM4_Mix, SM4_Mix (Lut_table bilan) o‘tkazish qobiliyatlari UCSM4 bilan solishtirildi va natijalar 11-jadvalda keltirilgan.

11-jadval.

O‘tkazish qobiliyatini taqqoslash natijalari

Amalga oshirish usuli	Jarayon	Kalit	Sikllar	Chastota /MHz	O‘tkazuvchanlik /Mbps
UCSM4	Shifrlash	O‘zgaruvchan	256	185	92.5
	Shifrni ochish	O‘zgaruvchan	256	185	92.5
	Shifrlash	O‘zgarmaydi	128	185	185
	Shifrni ochish	O‘zgarmaydi	128	185	185
ULSM4	Shifrlash	Ahamiyatga ega emas	256	435	217.5
	Shifrni ochish	Ahamiyatga ega emas	372	435	149.7
ULSM4_2 [mazkur ish]	Shifrlash	Ahamiyatga ega emas	256	435	225.4
	Shifrni ochish	Ahamiyatga ega emas	372	435	162.5
SM4_Mix	Shifrlash	Ahamiyatga ega emas	288	480	204.5
	Shifrni ochish	Ahamiyatga ega emas	404	480	134.7
SM4_Mix (Lut_table)	Shifrlash	Ahamiyatga ega emas	256	435	225.4
	Shifrni ochish	Ahamiyatga ega emas	372	435	162.5

O‘tkazuvchanlik maksimal chastota va SM4 algoritmini bajarish uchun zarur bo‘lgan iteratsiyalar soni bilan belgilanadi. Barcha raund kalitlarni saqlash uchun xotira muhim bo‘lganligi sababli, UCSM4 ning maksimal chastotasi 185 MGts bilan cheklangan UCSM4_2 kirish kalitlari o‘zgartirilganda shifrlash yoki shifrni hal qilish uchun 256 siklni va kirish kalitlari o‘zgarishsiz qolganda 128 tsiklni talab qiladi. Shunday qilib, UCSM4 ning maksimal o‘tkazuvchanligi 185 MGts ni tashkil qiladi.

XULOSA

SM4 algoritmi chiziqli kriptotahlil usuliga baholandi. Tahlil natijasida chiziqli kriptotahlil uchun SM4 algoritmining 23 raundiga $2^{126.4}$ ochiq matn va shifrlangan matn juftligi va $2^{121.7}$ vaqt murakkabligi zarurligi aniqlandi. Shuningdek, ko‘p o‘lchovli chiziqli kriptotahlilni amalga oshirish uchun esa 23-raundga $2^{122.3}$ ochiq matn va shifrlangan matn juftlari kerak bo‘lishi, vaqt murakkabligi esa $2^{122.5}$ ga

tengligi aniqlandi. Ushbu ishda o‘tkazilgan chiziqli kriptotahlillar hozirgi kunga qadar eng samarali hisoblanadi. MixColumns() akslantirishidan foydalanilganda, u chiziqli kriptotahlil jarayonida faqat tenglamalardagi noma’lumlar soniga ta’sir qilishi va chiziqlilik darajasiga va ularning ehtimoliga ta’sir qilmaydi.

SM4 algoritmi algebraik kriptotahlil usuliga baholanganda SM4 algoritmining 21 ta raundi uchun 2^{36} ta noma’lumli 12519 ta tenglama shakllantirish mumkinligi aniqlandi. Mazkur tenglamalar tizimini yechish murakkabligi 2^{108} ga ekvivalent ekanligi aniqlandi. SM4_Mix da esa noma’lumlar soni 2^{64} ta, yechimning murakkabligi esa 2^{192} ga teng bo‘ladi. Ikkala holatda ham tuziladigan tenglamalar soni bir-biridan farq qilmaydi. SM4 shifrlash algoritmi 22-raunddan keyin algebraik kriptotahlil usuliga bardoshli.

SM4 va SM4_Mix shifrlash algoritmlari tanlangan ochiq matnli kuchga asoslangan va differensial kriptotahlil usuliga baholanganda SM4 algoritmining 4 raundi uchun shifrlash kalitini izlashning murakkabligi $4 \times 2^4 \times 2^8 = 2^{14}$, SM4_Mix algoritmi uchun esa $16 \times 2^4 \times 2^8 = 2^{16}$ ekanligi aniqlandi.

Python dasturlash tilida SM4 shifrlash algoritmining akslantirishlarini amalga oshirish usullari o‘rganildi. Ushbu amalga oshirish usullari yordamida algoritmni amalga oshirishda vaqt bo‘yicha yuqori samaradorlikka erishish imkonini beradigan (100 000 blok uchun shifrlash vaqti 5,526601 soniya va shifrni ochish vaqti 5,759675 soniya) usul taklif qilindi. SM4_Mix algoritmida 100 000 blok uchun shifrlash vaqti 18,53468 soniyani, shifrni ochish vaqti esa 18,74289 soniyani tashkil qiladi. SM4_Mix (Lut_table) algoritmida 100 000 blok uchun shifrlash vaqti 5,234876 soniya, shifrni ochish vaqti esa 5,482364 soniya sarflanishi aniqlandi.

SM4 simmetrik blokli shifrlash algoritmi va uning modifikatsiya varianti SM4_Mixni apparatda amalga oshirishning optimal usuli sifatida taklif qilindi va taklif qilingan ULSM4_2 UCSM4 bilan solishtirganda yuqori maksimal o‘tkazish qobiliyatiga (shifrlash uchun 225,4 Mbit / s va shifrni ochish uchun 162,5 Mbit / s) egaligi aniqlandi. SM4_Mix (Lut_table bilan) SM4_Mix bilan solishtirganda yuqori maksimal o‘tkazish qobiliyatiga (shifrlash uchun 225,4 Mbit / s va shifrni ochish uchun 162,5 Mbit / s) egaligi ko‘rsatildi.

Mazkur ishda olingan natijalar shifrlash algoritmlarini ishlab chiqish, yangi akslantirish funktsiyalarini loyihalash va kriptotahlil usullarni qo‘llash uchun asos bo‘lib xizmat qilishi mumkin.

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

NATIONAL UNIVERSITY OF UZBEKISTAN

LIU LINGYUN

EVALUATION OF THE SM4 ENCRYPTION ALGORITHM USING CRYPTANALYSIS METHODS

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

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON PHYSICAL AND MATHEMATICAL SCIENCES

Tashkent-2024

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Commission at the Ministers of Higher Education, Science and Innovations of the Republic of Uzbekistan under number B2023.4.PhD/FM991.

Dissertation has been prepared at National University of Uzbekistan.

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

Scientific supervisor:	**Abdurakhimov Bakhtiyor Fayzievich** doctor of Physical and Mathematical Sciences, Professor
Official opponents:	**Kabulov Anvar Vasilovich** doctor of Technical Sciences, Professor
	Nie Yang PhD, professor, Jining Normal University, China
Leading organization:	**Termez State University**

Defense will take place "29" august 2024 at 1400 ft the meeting of Scientific Council number DSc.03/30.12.2019.FM.01.02 at National University of Uzbekistan. (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 227-12-24, fax: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

Dissertation in possible to review in Information-resource centre at National University of Uzbekistan (is registered №78). (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 246-02-24).

Abstract of dissertation sent out on "16" august 2024 year
(Mailing report №3 on "24" june 2024 year)

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

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

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

INTRODUCTION (abstract of PhD thesis)

Importance and necessity of the dissertation topic. Globally, special importance is attached to assessing the cryptographic strength of symmetric block encryption algorithms. In particular, particular importance is attached to the evaluation of cryptanalysis methods aimed at determining the secret key used in the encryption process, and depending on the features of the mathematical reflections used in the algorithm, the steps of the reflection algorithm, as well as independently of the mathematical features and stages of the reflections. The study of the mathematical properties of the transformations used in the encryption algorithms, the issues of evaluating the algorithms against existing crypto-attacks are the object of scientific research conducted in the fields of information security, cryptography, cryptanalysis, and applied mathematics. Therefore, given the speed of development of technology and science, special attention is paid to the constant assessment of cryptanalysis methods for compliance with the stability requirements of standard encryption algorithms.

Currently, information security in the world is implemented using software and hardware, so the standard cryptographic encryption algorithms and protocols used in these tools are widely studied for the tolerance requirements of cryptanalysis methods. Symmetric encryption algorithms are widely used to ensure confidentiality in the storage, processing and transmission of information. In addition, it is important to design and optimize the hardware structure for the computation speed of the SM4 symmetric block cipher algorithm and determine its robustness. For this reason, the analysis of standard symmetric encryption algorithms and the ongoing assessment of their resistance to modern cryptanalysis methods are among the targeted scientific research.

In the Republic of Uzbekistan, as a scientific and practical application of fundamental sciences, much attention is paid to such current areas as information security, the creation of stable cryptographic algorithms in the field of cryptology and the assessment of their security. Significant results are achieved in the use of symmetric block encryption algorithms to ensure confidentiality and integrity of information, the creation and application of methods and algorithms aimed at evaluating symmetric block encryption algorithms to cryptanalysis methods. The measures to approve the strategy “Digital Uzbekistan - 2030” and its effective implementation define tasks, including “ensuring the information security of departmental digital infrastructure, as well as the protection of electronic data and documents.” When implementing these tasks, it is important to compare standard encryption algorithms with cryptanalysis methods and apply the results obtained in practice.

Decree of the President of the Republic of Uzbekistan No. PF-60 dated January 28, 2022 “On the Development Strategy of the new Uzbekistan for 2022-2026”, No. PQ-4708 dated May 7, 2020 Resolution “On measures to improve the quality of education in the field of mathematics and the development of scientific research ”, No. PF-5847 dated October 8, 2019 “Development of the higher education system of the Republic of Uzbekistan until 2030” Resolution No. PQ-3682 dated April 27,

2019 “On measures to further improve the system for introducing innovative ideas, technologies and projects” and 2021 This dissertation research serves to a certain extent in the implementation of the tasks defined in Resolution No. PF-6198 of April 1 “On improving the system of public management of the development of scientific and innovative activities” and other regulatory documents related to this activity.

Alignment of the study with the key priorities in the advancement of science and technology in the republic. This research is the fourth segment of the country's science and technology advancement efforts. It was conducted under the priority domain of "Advancement of Information and Communication Technologies."

The level of study of the problem. Numerous researchers, such as Ji W., Hu L., Schneier B., Liu F., Ferguson N., Knudsen L., Hang W., Huili C., Xiaoqing L. V., Dodis Y., Matsui M., Kim T., Courtois N., Zhang W., Harris N., Shamir A., Su B.Z., Wu W.L., Bigham E., Kelsey J., Cho J., Jakimoski G., Oleynikov R., Sun Y. Ishchukova E., Hu W., Babenko L., Shan W. and Kazimirov O., have undertaken investigations into the cryptanalysis of symmetric block encryption algorithms and the creation of robust symmetric block ciphers. They have conducted scientific inquiries focused on the development of encryption algorithms, the establishment of durable cryptographic transformations, and the assessment of these transformations against various cryptanalysis methods.

Worldwide, many cryptanalytic studies have been conducted on the SM4 algorithm by many cryptographers and cryptanalysts. In particular, Kim T. et al. presented e present a linear attack and a differential attack on a 22-round reduced SMS4 and a boomerang and a rectangle attack on an 18-round reduced SMS4. On SM4, Wang and Du et al. initially introduced the chosen plaintext power attack. Subsequently, Shan and Chen et al. expanded upon this attack by leveraging specific plaintexts to widen its scope on SM4. In pursuit of enhancing correlation in power analysis, Hu et al. proposed a comprehensive adaptively chosen-plaintext approach. Further refining the technique to accommodate both non-adaptive and adaptive scenarios, Maamar O et al. contributed significantly. These methodologies find applicability in the examination of various grouping algorithms like SM4 and AES.

Zhang et al. employs a byte-oriented random fault model and incorporates differential analysis techniques. The attack method theoretically requires only 32 incorrect ciphertexts to fully recover the 128-bit seed key of SM4. Hu et al.by attacking multiple locations where information may be leaked, the information leakage point is successfully found, and the key for the first round, the key for the 2nd, 3rd, and 4th rounds are successfully recovered, and then the 128bit source key is deduced. Wang S. et al. employed two means - the Hamming distance model and the bit model - to model power. WANG M. et al. proposed a selective-plain text power analysis attack against SMS4 using polled output as intermediate data. Shan W. et al. introduces le a CPA selective plain text method against SM4 block ciphers. DPA attack of Jiazhe C. et al., a reasonable choice of plaintext can minimize the effect of variable input bits on output bits in the linear transformation of SM4, thus providing an effective side-channel attack on SM4. Hu W. et al. divided the track

acquisition process into two phases. Adaptive selection of specific plaintexts corresponding to high signal-to-noise ratio traces completes the attack with fewer traces. Heuser A. et al. it was shown that leakage modelling can be reduced to some extent by mathematical methods. Currently, there is not much research on SM4 software implementation methods. At present, although many researchers have studied the hardware implementation structure of the SM4 algorithm, most of them focus on the design and optimization of the hardware structure for the computing speed of the SM4 algorithm, and there is still a large redundancy. It can also be designed and optimized with area throughput as the main constraint.

The connection of the dissertation research with the research plans of the higher education institution where the dissertation was completed. Dissertation research was conducted within within the framework of the project “Research and development of stream encryption algorithms” No. UZB-Ind-2021-98 in accordance with the research plan of the National University of Uzbekistan.

The aim of the research work is to evaluate the stability of the symmetric encryption algorithm SM4 and its modified version SM4_Mix using cryptanalysis methods and to determine the optimal methods for software and hardware implementation.

Tasks of the research:

evaluation of the tolerance of SM4 symmetric block encryption algorithm using linear cryptanalysis method;

evaluation of the tolerance of SM4_Mix algorithms, a modification of the SM4 symmetric block encryption algorithm, using the linear cryptanalysis method;

evaluation of the tolerance of SM4 symmetric block encryption algorithm and its modification variant SM4_Mix algorithms using algebraic cryptanalysis method;

evaluation of the tolerance of SM4 symmetric block encryption algorithm and modification variant SM4_Mix algorithms using the power and differential analysis of chosen plaintexts cryptanalysis method;

determining optimal methods of software and hardware implementation of SM4 symmetric block encryption algorithm and its modification variant SM4_Mix.

The object of research: symmetric encryption algorithm and cryptanalysis processes.

The subject of the research is the SM4 symmetric encryption algorithm and its modification variant SM4_Mix and methods of evaluating using cryptanalysis methods.

Research methods. Applied cryptography and cryptanalysis methods, number theory, probability theory, comparative comparison, and methods of conducting experiments using object-oriented programming tools were used in the research process.

The scientific novelty of the research is as follows:

the SM4 and SM4_Mix encryption algorithms were evaluated using the linear cryptanalysis method and the optimal approximation equations required to be used in the linear analysis for the 23-round SM4 algorithm to be used in the linear

analysis, N =$2^{126.4}$ pairs of plaintext and ciphertext were used for the attack, the need was determined;

in the process of assessing the stability of the SM4_Mix algorithm using the linear cryptanalysis method, it was established that the number of unknowns in the generated equations is 4 times higher than that of the SM4 algorithm, the level of linearity and their probability do not differ, that is, $2^{-60.5}$ for 20 rounds;

in the process of assessing the tolerance of the SM4_Mix algorithm using linear cryptanalysis, it was found that the number of unknowns in the generated equations increases compared to the SM4 algorithm, and the level of linearity and their probability do not differ;

during the evaluation of the SM4 and SM4_Mix encryption algorithms by the method of algebraic cryptanalysis, 2^{36} algebraic equations with a complexity of 2^{108} were generated in 21 rounds of the SM4 algorithm; in 21 rounds of the SM4_Mix algorithm, 2^{64} algebraic equations were generated with a solution complexity of 2^{192} and has been proven that the algorithm's resistance to algebraic cryptanalysis increases when using the MixColumns() transformation;

during the evaluation of the SM4 and SM4_Mix encryption algorithms using the cryptanalysis method of force and differential analysis of selected plaintexts, it was found that the complexity of finding the encryption key in 4 rounds of the SM4 algorithm is equal to 2^{14}, for the SM4_Mix algorithm it is equal to 2^{16};

optimal methods for implementing the L- and S-transformation of the SM4 algorithm are determined, for implementing the SM4 and SM4_Mix algorithms in hardware, with high throughput, taking up less space, i.e. 26.808 μm², and fast and efficient software methods are proposed that require 5.234876 seconds to encrypt 100,000 data blocks and 5.482364 seconds to decrypt

The practical result of the research is as follows:

Software tools for optimal implementation of SM4 and SM4_Mix symmetric encryption algorithms were developed;

A software tool for forming algebraic equations for the s-block table of the SM4 encryption algorithm has been developed.

Reliability of research results. The credibility of the dissertation findings is based on precise mathematical reasoning, supported by the results of multiple studies, as well as practical and experimental analyses of cryptographic algorithms utilizing various methods of cryptanalysis.

Scientific and practical significance of research results. The research findings evaluate the SM4 symmetric block encryption algorithm using linear, algebraic, power and differential analysis of chosen plaintexts cryptanalysis methods, which holds significant scientific importance.

The results have practical significance because they highlight the potential use of cryptanalysis methods and cryptographic attributes of transformations in evaluating modern encryption algorithms. This knowledge can be used to develop new encryption algorithms, design innovative transformation functions, and explore the application of cryptanalysis methods.

Implementation of the research results. Scientific results on the evaluation

of the SM4 algorithm using cryptanalysis methods are put into practice in the following areas:

software for optimal methods for implementing the SM4 and SM4_Mix encryption algorithms developed in the dissertation work was experimentally tested in the process of transmitting information in the communication and telephone networks of Uzbektelecom JSC Samarkand city communication line (“Reference number 61-03-12/485 dated April 4 2024 of the Samarkand branch of Uzbektelecom). In the process of applying scientific results, the proposed software tool for the optimal implementation of the SM4 encryption algorithm allows you to encrypt 2.21 MB of open data and reverse 2.12 MB of encrypted data in 1 second, the proposed method for software implementation of the software tool of the SM4_Mix algorithm allows you to encrypt 2.33 MB of open data and reset 2.22 MB of encrypted data in 1 second;

from the optimal approximation equations for the 23rd round SM4 algorithm developed in the thesis used in laboratory tests to evaluate the compatibility, accuracy and efficiency of applications for assessing the security of commercial cryptography applications, cryptography in networks and information systems in Inner Mongolia Wangxin Information Security Service Co. , Ltd (reference WXSEC20240315001, March 15, 2024) As a result of applying scientific results, it was found that to carry out a linear cryptanalysis attack on the SM4 algorithm, 2126.4 pairs of plaintext and ciphertext are needed, and the results obtained allowed us to achieve effective results in the process of assessing the stability of the algorithm SM4 encryption to the linear cryptanalysis method;

optimal methods for software implementation of the SM4 encryption algorithm developed in the thesis, including methods for optimal implementation of L- and S-reflections of the SM4 algorithm, methods for implementing reflections of the SM4 encryption algorithm in the Python programming language, a method describing the S-box as a one-dimensional table, an effective method for performing a cyclic operation left shift, methods for optimal implementation of the encryption algorithm in the Python programming language, which achieved time savings compared with other implementation methods, applied to the digital science project jsky2021098 "SM4, Algorithm Research" was carried out by the School of Electronic and Information Engineering, Jining Normal University, Jining Normal University (Jining Normal University Certificate No. 20240315-001 dated March 15, 2024). As a result of applying scientific results, the time spent on encrypting 100,000 data blocks was 5.526601 seconds, and the decryption time was 5.759675 seconds, and the proposed implementation methods improved the performance of the SM4 encryption algorithm.

Approval of research results. The results of this research were discussed at 3 international and 2 national scientific-practical conferences.

Publication of research results. A total of 26 scientific works were published on the subject of the dissertation, including 8 articles in scientific publications recommended for publication of the main scientific results of dissertations by the Higher Attestation Commission of the Republic of Uzbekistan, including 2 articles

in publications indexable in the Scopus database, international conference 3, local conference 2, foreign journal 10. Also, certificates of registration of 3 software tools created for EHM were received.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, three chapters, conclusion, references and appendix. The volume of the thesis is 101 pages.

THE MAIN CONTENT OF THE DISSERTATION

In the introduction. The introduction of the dissertation will highlight the importance and relevance of the chosen topic of research. It will demonstrate how the research aligns with the priority directions of science and technology development in the Republic of Uzbekistan. The introduction will also define the goals and tasks of the research, as well as the object and subject of investigation. The obtained results will be thoroughly explained to justify their reliability and highlight their theoretical and practical significance. Additionally, the introduction will provide information on the progress of research implementation, published works, and the dissertation structure.

The first chapter of the dissertation, entitled "**Feistel network-based encryption algorithms. SM4 encryption algorithm and the results of its evaluation using cryptanalysis methods**" describes encryption algorithms developed based on the Feistel network, as well as the SM4 encryption algorithm. The main transformations used in the algorithm and the results of cryptanalysis of this algorithm are presented.

Most modern symmetric block ciphers use a Feistel network, a Feistel structure that first appeared in IBM's Lucifer encryption algorithm (a predecessor of the DES algorithm) proposed by Horst Feistel and Don Coppersmith. There are many types of encryption algorithms developed using the Feistel structure, DES, MISTY1, and SM4 all use the Feistel structure. Also, algorithms using this network are Blowfish, Camellia, CAST-128, FEAL, ICE, KASUMI, LOKI97, Lucifer, MARS, MAGENTA, RC5, TEA, Triple DES, Twofish, XTEA, GOST_28147-89, CAST-256, MacGuffin, RC2 , RC6 and other algorithms are considered.

SM4 is the basic block cipher used in the Chinese wireless LAN security standard WAPI (Wireless LAN Authentication and Privacy Infrastructure), which is the first commercial cryptographic algorithm announced by the Chinese government in 2006.In 2012 it was announced as the standard for commercial block ciphers in China. In 2021 it became part of the international standard ISO/IEC. SM4 has received a lot of attention in the cryptographic field from the beginning of its appearance. For an algorithm, the security of the algorithm needs to be considered, which requires the algorithm to be analyzed using various analysis methods.

The design goal of the SM4 algorithm is to provide a highly secure, efficient and easy-to-implement block cipher scheme. It employs a 128-bit key and block size, executing encryption and decryption via a 32-round iterative process that involves basic operations like substitution and XOR. SM4 has high security, has

passed a variety of cryptographic security analyzes and evaluations, and is widely recognized and accepted.

SM4 has been effectively cryptanalyzed by cryptanalysts using various cryptanalysis methods.

Some of the results of cryptanalysis performed on the algorithm are shown in Table 1.

Table 1.

Results of cryptanalysis performed on the SM 4 algorithm

Methods used	Attacked round	Time spent	Amount of data used	Required memory
Cryptanalysis with linear cryptanalysis	24	$2^{122.6}$	$2^{122.6}$	2^{85}
Multivariate linear cryptanalysis	23	$2^{122.7}$	$2^{122.6}$	$2^{120.6}$
Differential cryptanalysis	23	$2^{126.7}$	2^{117}	2^{130}
Matrix dimensional cryptanalysis	18	$2^{110.77}$	2^{127}	2^{130}
Advanced differential cryptanalysis	17	2^{132}	2^{117}	-
Improved linear cryptanalysis	14	$2^{120.7}$	$2^{123.5}$	2^{73}
Integral cryptanalysis	14	$2^{96.5}$	2^{32}	-

The second chapter of the dissertation entitled **“Evaluation of the SM4 encryption algorithm using cryptanalysis methods”** presents the results of the evaluation of the SM4 encryption algorithm and its modified variant SM4_Mix algorithm based on linear, algebraic, power and differential analysis of chosen plaintexts cryptanalysis methods.

Linear cryptanalysis stands out as a crucial technique in the examination of symmetric-key cryptographic primitives. This method primarily focuses on establishing linear approximations among plaintext, ciphertext, and the key. When a cipher exhibits non-random permutation behavior under linear cryptanalysis, it becomes possible to construct a distinguisher or even initiate a key recovery attack by incorporating additional rounds. The process involves making educated guesses for the subkeys of appended rounds, decrypting ciphertexts and/or encrypting plaintexts using these subkeys to calculate the intermediate state at the ends of the distinguisher. If the subkeys are accurately guessed, the distinguisher should be valid; otherwise, it will fail. Linear cryptanalysis has been employed in the analysis of various ciphers.

Regarding the efficacy across all previous SM4 attacks in terms of the number of rounds, the most effective key recovery methods are linear cryptanalysis and differential cryptanalysis. Both approaches rely on 19-round distinguishers. Our primary motivation is to enhance the attacks on SM4 by seeking a superior distinguisher. Consequently, our focus centers on exploring linear approximations for SM4.

The most effective previous linear attacks have focused on 19-round linear approximations. In response, we introduce a novel search algorithm specifically designed for iterative linear approximations over a small number of rounds in SM4. This involves systematically expanding the partial linear approximation table of the S-box. Initially, it is demonstrated that there are no one-round or two-round iterative linear approximations for SM4. Subsequently, certain properties are derived for the iterative linear approximations of 3-round SM4. Leveraging these properties, our search algorithm is applied to obtain a 19-round linear approximation with a bias of $2^{-57.3}$ and a 20-round linear approximation with a bias of $2^{-60.5}$. A comparison of our identified linear approximations with previous ones is presented in Table 2. Notably, our linear approximations emerge as the most effective to date.

Table 2.

Overview of Linear Approximations for SM4.

Reference	Bias (probability)	Rounds
[29]	$2^{-62.27}$	19
[14]	2^{-58}	19
[14]	2^{-61}	20
this work	$2^{-57.3}$	19
this work	$2^{-60.5}$	20

The most effective prior attacks have demonstrated efficacy up to 23 rounds for SM4. Leveraging our identified 20-round linear approximation for SM4, we introduce a key recovery attack targeting 24-round SM4, which currently stands as the most potent attack based on the number of rounds for SM4. Additionally, we employ the newly established 19-round linear approximation to launch an attack on 23-round SM4, thereby enhancing the effectiveness of the best previous linear attack on 23-round SM4. An overview of our attacks and those previously conducted on SM4 is provided in Table 3.

Theorem 1. To construct the 19-round linear approximation, it is necessary for the input masks of the T functions in two consecutive active rounds to be identical.

Proof. Let Γ_{in}^{i} and Γ_{in}^{i} $(i = 1,\cdots,6)$ represent the input and output masks of the T functions in the six-round linear approximation with the pattern $0 - 0 - 2 - 2 - 0 - 0$. Then $\Gamma_{in}^{3} \oplus \Gamma_{out}^{1} \oplus \Gamma_{in}^{2} = \Gamma_{in}^{4} \oplus \Gamma_{out}^{5}$, $\Gamma_{in}^{4} \oplus \Gamma_{out}^{6} \oplus \Gamma_{in}^{5} = \Gamma_{in}^{3} \oplus \Gamma_{out}^{2}$. Since $\Gamma_{in}^{j} = \Gamma_{out}^{j} = 0$ for $j = 1,2,5,6$. As a result, $\Gamma_{in}^{3} = \Gamma_{in}^{4}$. Theorem 1 is proved.

Table 3.

Overview of Attacks on SM4

Type of cryptanalysis methods	Number of rounds	Time (T: sec)	Data (D)	Reference
Rectangle	16	2^{116}	2^{125}	[28][30]
Rectangle	14	$2^{87.69}$	$2^{107.89}$	[22][23]
Rectangle	18	$2^{112.83}$	2^{124}	[15]
Integral	13	2^{114}	2^{16}	[11]
Impossible Differential	16	$2^{96.07}$	$2^{117.06}$	[23]
Boomerang	18	$2^{116.83}$	2^{120}	[15]
Differential	21	$2^{126.6}$	2^{118}	[31]
Differential	23	$2^{126.7}$	2^{118}	[18]
Differential	22	$2^{125.71}$	2^{118}	[15]
Differential	22	$2^{112.3}$	2^{117}	[17]
Linear	22	2^{117}	$2^{118.4}$	[16]
Linear	22	$2^{109.86}$	2^{117}	[15]
Linear	23	2^{122}	$2^{126.54}$	[29]
Multiple Linear	22	$2^{119.75}$	2^{112}	[32]
Multidimensional Linear	23	$2^{127.4}$	$2^{126.6}$	[19]
Multidimensional Linear	23	$2^{122.7}$	$2^{122.6}$	[29]
Linear	23	$2^{121.7}$	$2^{126.4}$	this work
Multidimensional Linear	23	$2^{122.5}$	$2^{122.3}$	this work

It was also considered how the results of this cryptanalysis could be if instead of the cyclic left-shift reflection used in the SM4 algorithm, the MixColumns() linear reflection used in the AES algorithm was used.

In the MixColumns representation, the state column elements are expressed as coefficients of a polynomial not larger than the third degree, given in this polynomial algorithm: $g(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ multiplied by mod x^4+1 to the polynomial.

We can see that using the MixColumns() transformation instead of the cyclic shift left operations used in the SM4 encryption algorithm results in 4 bits per bit being generated. In the shift operation, it is equal to one bit. From this, it can be concluded that when MixColumns() transformation is used, it affects only the number of unknowns in the equations in the process of linear cryptanalysis, and does not affect the degree of linearity and their probability.

In the algebraic analysis modeling of the SM4 cipher, it is important to highlight that the primary transformation employed to construct the system of

equations is a nonlinear substitution within the S-boxes. Represent the total number of compositions of input and output block bits as t. Consequently, there are at least $t - 2^s$ linearly independent equations that are valid with a probability of 1.

As an example, the Boolean nonlinear equations for an $s \times s$-bit S-box are defined as follows (Equation 1):

$$\sum_{i,j,k=0}^{s-1} \alpha x_i y_j y_k + \sum_{i,j,k=0}^{s-1} \beta x_i x_j y_k + \sum_{i,j=0}^{s-1} \gamma x_i y_j + \sum_{i,j=0}^{s-1} \delta y_i y_j + \sum_{i=0}^{3} \lambda x_i + \sum_{i=0}^{3} \omega y_i + \eta = 0 \quad \textbf{(1)}$$

where each of $\alpha, \beta, \gamma, \delta, \lambda, \omega, \eta$ are binary coefficients;

x_i and y_i correspond to the i-th bit of the input and output vectors of the S-box, respectively;

s represents the length of the input and output vectors.

The equation (2) is utilized to compute the number of possible equations with a degree of 3 or less:

$$t = \binom{2s}{3} + \binom{2s}{2} + 2s + 1 \quad \textbf{(2)}$$

In the case of the SM4 cipher with an 8 × 8-bit S-box, the total number of monomials, denoted as t, is obtained as follows:

$$t = \binom{16}{3} + \binom{16}{2} + 16 + 1 = 697 \quad \textbf{(3)}$$

Consequently, it is feasible to identify $r \geq t - 2^8 = 441$ linearly independent cubic equations. The system of degree 3 Boolean equations for the SM4 substitution box comprises the equations outlined in Figure 1.

x3y0+x2y7+x2y1+x1y7+x1y3+x1y2+x1y1+x1y0+y6+y5+y4+y3+y2+y1+y7+y3+y1+y0+x7x6x5+x7x6x3+x7x6x2+x7x6x1+x7x6+x7x5x4+x7x5x3+x7x5x2+x7x5+x7x4x1+x7x4x0+x7x4+x7x3x0+x7x2x1+x7x2+x7x1+x7x0+x7+x6x5x4+x6x5x3+x6x5x2+x6x5+x6x4x2+x6x4x1+x6x4+x6x1x0+x6x1+x6x0+x6+x5x4x0+x5x3+x5x2x1+x5x2x0+x5x2+x5x1+x5x0+x5+x4x3x2+x4x3+x4x1x0+x3x2x0+x3x1x0+x2x1x0+x2+x1x0+x0=0

x3y2+x3y1+x2y7+x2y6+x2y5+x2y4+x2y3+x2y1+x2y0+x1y5+x1y4+x1y2+y6+y5+y1+y0+x7x6x4+x7x5x4+x7x5x3+x7x4x1+x7x4x0+x7x3+x7x2x0+x7x1x0+x7x1+x7+x6x5x4+x6x5x2+x6x5x0+x6x5+x6x4x3+x6x4x2+x6x4x0+x6x3x0+x6x3+x6x2x1+x6x1x0+x6x1+x6+x5x4x3+x5x4x2+x5x4x1+x5x4x0+x5x3x2+x5x3+x5x2x0+x5x2+x4x3x0+x4x2x0+x4x1x0+x4x1+x4x0+x4=0

x3y3+x3y1+x2y3+x2y2+x1y7+x1y6+x1y4+x1y3+x1y0+y5+y7+y5+y4+y3+y2+y1+y0+x7x6x5+x7x6x3+x7x6x2+x7x6x1+x7x6x0+x7x6+x7x5x4+x7x5x3+x7x5x2+x7x5x1+x7x5x0+x7x5+x7x4x3+x7x4x2+x7x4+x7x3x0+x7x3+x7x2x0+x7x2+x7x1x0+x7x1+x7x0+x6x5x0+x6x5+x6x4x3+x6x4x1+x6x4+x6x3x2+x6x3x0+x6x2x1+x6x2x0+x6x1+x6x0+x6+x5x4x3+x5x4x2+x5x4x1+x5x4x0+x5x3x2+x5x3x0+x5x2x0+x5x2+x5x1x0+x5x1+x5+x4x2+x4x1x0+x4+x3x2x1+x3x1x0+x3x1+x2x1x0+x1x0+x1=0

…..

Figure 1. Degree 3 Boolean equations system for SM4 substitution box.

The SM4 cipher's S-box transformation is expressed through 441 linearly independent equations, featuring a total number of monomials not exceeding 697. One round of the SM4 encryption algorithm, considering that the only nonlinear operation is substitution in S-boxes, and other transformations result in bit permutations, can be delineated as a system of 1764 cubic linearly independent equations with 64 unknowns (round key rk and S-boxes output vector). For the full-

round version of SM4 (32 rounds), a set of 56448 cubic equations with 2048 unknowns was formulated (32 rk_i and 32 S-boxes output vector).

It is also possible to form a degree 2 system of equations for the S-box substitution table of the SM4 encryption algorithm. Degree 2 Boolean equations for the SM4 substitution box comprises the equations outlined in Figure 2.

x4y0+x3y6+x3y2+x3y0+x2y6+x2y4+x2y3+x2y0+x1y7+x1y5+x1y4+x1y3+x1y0+y7+y5+y4+y3+y2+y0
+y6+y5+x7x6+x7x5+x7x4+x7x3+x7x2+x7x1+x6x4+x6x2+x6x1+x5x4+x5x3+x5x2+x5x1+x4x2+x4x0+
x4+x3x2+x3x1+x3x0+x2x0+x2=0

x4y1+x3y4+x3y2+x3y1+x2y5+x2y4+x2y3+x2y1+x2y0+x1y7+x1y5+x1y2+x1y1+y6+y4+y3+y1+y6+y3
+x7x6+x7x5+x7x2+x7x1+x6x5+x6x2+x5x4+x5+x4x0+x4+x3x1+x3x0+x2x1+x2x0+x1x0+x0=0

x4y2+x3y5+x3y4+x3y2+x3y0+x2y7+x2y6+x2y5+x2y4+x2y3+x2y2+x2y1+x2y0+x1y4+x1y3+x1y2+x1y
0+y4+y3+y2+x7x4+x7x2+x7x1+x7x0+x7+x6x5+x6x4+x6x3+x6x1+x6+x5x4+x5x0+x4x2+x2x0+x2+x1
x0=0

x4y4+x4y3+x3y1+x2y7+x2y4+x2y2+x2y1+x1y6+x1y5+x1y3+x1y1+x1y0+y7+y5+y3+y2+y6+y5+y4+y
2+y0+x7x5+x7x4+x7x2+x6x5+x6x4+x6x3+x6x0+x5x3+x5x1+x5+x4x0+x3x1+x2x0=0

x4y5+x4y3+x3y7+x3y1+x3y0+x2y7+x2y5+x2y4+x2y3+x2y1+x2y0+x1y7+x1y5+x1y4+x1y3+x1y2+x1y
0+y7+y6+y5+y4+y2+y0+y5+y3+y2+y1+x7x4+x7x0+x7+x6x5+x6x3+x6x1+x6x0+x6+x5x4+x5x2+x5x1
+x5+x4x3+x4x1+x4x0+x4+x3x1+x3x0+x3+x2+x1=0

x4y6+x3y6+x3y5+x3y4+x3y2+x3y1+x2y7+x2y4+x2y2+x2y1+x2y0+x1y6+x1y5+x1y4+x1y3+x1y1+y6
+y2+y1+y7+y3+y1+x7x5+x7x4+x7x2+x7x1+x7x0+x6x4+x6x0+x6+x5+x4x1+x4x0+x3x2+x3x1+x3x0+
x2x1+x2+x1x0+x0=0

……..

Figure 2. Degree 2 Boolean equations system for SM4 substitution box.

Theorem 2. The algorithm's resistance to algebraic cryptanalysis increases when MixColumns() transformation is used instead of left-shifted cyclic transformation.

Proof. Data on the number of nonlinear equations, the number of unknowns, and the complexity of solving for the SM4 encryption algorithm are given in Table 4 below.

From this table, we can see that the SM4 encryption algorithm is robust to the algebraic cryptanalysis method after round 22.

Table 4

Characterization of algebraic equations in rounds of the SM4 algorithm

Round	Linearly independent equations	Unknowns	Complexity
1	39	2^6	2^{18}
5	2535	2^{12}	2^{36}
9	5031	2^{18}	2^{54}
13	7527	2^{24}	2^{72}
17	10023	2^{30}	2^{90}
21	12519	2^{36}	2^{108}
25	15015	2^{42}	2^{120}

Algebraic cryptanalysis can also be performed for the SM4_Mix variant of the algorithm. As noted in linear cryptanalysis, the MixColumns() transformation

affects the number of unknowns in the discount. That is, in algebraic analysis, most of the equations formed for the bits in the output of s_box are involved in expressing the output from MixColumns() transformation. Table 5 lists the number of variables in the equations representing the rounds for the SM4_Mix variant of the algorithm and the complexity of solving them.

It can be concluded from this table that if the MixColumns() transformation is used instead of the cyclic push transformation used in the SM4 algorithm, the tolerance of the algorithm to algebraic cryptanalysis increases. For example, the number of unknowns in the equation representing 21 rounds of the SM4 algorithm is 2^{36}, and the complexity of the solution is 2^{108}, while in SM4_Mix, the number of unknowns is 2^{64}, and the complexity of the solution is 2^{192}. The number of equations to be formulated in both cases does not differ.

Table 5

Characterization of algebraic equations in rounds of the SM4_Mix algorithm

Round	Linearly independent equations	Unknowns	Complexity
1	39	2^{6+4}	2^{30}
5	2535	2^{20+4}	2^{72}
9	5031	2^{30+4}	2^{112}
13	7527	2^{40+4}	2^{132}
17	10023	2^{50+4}	2^{162}
21	12519	2^{60+4}	2^{192}
25	15015	2^{70+4}	2^{222}

Also, the SM4 encryption algorithm was evaluated against selected plaintext strength-based and differential cryptanalysis methods. If the attack is performed in a temporary manner, the entire 128-bit key of SM4 can be completely recovered by two or four rounds of analysis. This approach has several advantages over traditional chosen plaintext attacks.

The chosen plaintext attack on SM4, involves selecting specific plaintexts with defined constraints to make the output res after the linear transformation (L) fixed. Subsequently, the round output X_{i+4} is chosen as the target for the attack ($X_{i+4} = X_i \oplus res$, where X_i is known random value and res is the fixed unknown value). Through power analysis, the fixed value res is determined, leading to the deduction of the round key. The overall key recovery for SM4 involves sequentially executing the chosen plaintext attack on the first four rounds.

In contrast to the earlier chosen plaintext attack, the integrated round reduction attack presented in this work exhibits clear advantages in terms of the number of required rounds for the attack, the choice of attack points, and the frequency of trace collection.

As shown in Table 6, this combination attack cuts the number of attack rounds in half, requires only two sets of traces, which is a significant improvement over previous attacks that involve a larger selection of plaintexts, and improves the overall attack efficiency. Additionally, focusing on the S-box output as the point of

attack instead of the front XOR or L-transposition and circular output effectively increases the attack's success rate. Moreover, the total number of traces required to recover the keys of the first four rounds of this attack (4 × N, where N is the number of traces for one successful attack) is significantly lower than the corresponding requirement (16 × N). While the total number of lanes is also 4×N, this combo attack achieves this in just two rounds and two sets of lanes, reducing both lane collection time and overall attack time. Finally, the complexity of the key search space is less than previous plaintext attacks.

When this cryptanalysis is carried out for the SM4_Mix option, it is observed that the level of differential differences is 4 times higher in the MixColumns() transformation, and the complexity is also 4 times higher compared to the SM4 algorithm.

Table 6.
Overview of Attacks on SM4

Attack Methods	The Intermediate Value of Power Attack	The Number of Tracing Collection Instances	The Total Number of Traces	Key Search Space Complexity
[62]	L transformation for rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
[63]	Round output of rounds 1, 2, 3, and 4	4	$4 \times N$	$4 \times 4 \times 2^8$
[64]	Round output of rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
[65]	Round output of rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
[79]	The S-box output of 2th and 4th rounds	2	$4 \times N$	$(4 \times 2^4 \times 2^8) \times 2$
SM4	The S-box output of 2th and 4th rounds	2	$4 \times N$	$(4 \times 2^4 \times 2^8)$
SM4_Mix	The S-box output of 2th and 4th rounds	2	$16 \times N$	$(16 \times 2^4 \times 2^8)$

In the third chapter of the dissertation, entitled "Development of optimal methods of software and hardware implementation of the SM4 encryption algorithm", methods of software and hardware implementation of the SM4 encryption algorithm and its modified variant SM4_Mix algorithm were studied and optimal implementation methods were proposed.

In the Python programming language, substitution tables (S-box) can be represented in three ways. These are in the form of dictionary view (Sbox_dict), 1 (Sbox_Table1) and 2 (Sbox_Table1) dimensional arrays. According to these methods of expression, the methods of referring to these tables also differ.

According to the form of representation of the substitution table, the functions to refer to them are as follows:

(1) A reference function for a state expressed in a dictionary view;
(2) A reference function for a state expressed as a 1-dimensional array;
(3) A reference function for a state expressed as a 2-dimensional array.

The values of the time taken to refer the substitution table for 10,000,000 random 32-bit values using the above program code are shown in Table 7 below.

The data in Table 7 indicates that employing a 1-dimensional array to represent substitution tables in the Python programming language results in significantly less time consumption compared to using a dictionary or a 2-dimensional array for representation.

Table 7

The values of the time taken to refer the substitution table for 10,000,000 random 32-bit values

No.	The representation method of S_box	A reference function	Time spent (sec)
1.	dictionary view (Sbox_dict)	def tau_dict(input: int) -> int	16.1635637283325
2.	1 dimensional arrays (Sbox_Table1)	def tau1(input: int) -> int	12.391227006912 2
3.	2 dimensional arrays (Sbox_Table2)	def tau2(a)	14.378753662109 3

The cyclic shift left operation can also be expressed in different ways in the Python programming language. Python programming language representations of these methods and the MixColumns() representation of the SM4_Mix algorithm are given below.

(1) 1st method operation cyclic shift left;

```
def left_shift_1(a: int, n: int) -> int:
        for i in range(n):
            a <<= 1
        if a // 0x100000000 == 1:
            a %= 0x100000000
            a += 1
        return a
```

(2) 2nd method operation cyclic shift left;

```
def left_shift_2(a:int, n:int):
    size=32
    n =n% 32
        return (a << n) | (a >> (size - n)) &0xffffffff
```

(3) 3rd method operation cyclic shift left;

```
def left_shift_2(a:int, n:int):
```

```
        size=32
        n =n% 32
    return (a << n) ^ (a >> (size - n)) &0xffffffff
```

(4) MixColumns() with Lut_table;

```
import time
def mixColumns(input):
    a = input // 0x01000000
    b = (input & 0x00ff0000) >> 16
    c = (input & 0x0000ff00) >> 8
    d = input % 0x100
    a1=mul2[a] ^ mul3[b] ^ c ^ d
    b1=a ^ mul2[b] ^ mul3[c] ^ d
    c1=a ^ b ^ mul2[c] ^ mul3[d]
    d1=mul3[a] ^ b ^ c ^ mul2[d]
```

(5) MixColumns();

```
def gmul(a, b):
 if b == 1:
  return a
 tmp = (a << 1) & 0xff
  if b == 2:
 return tmp if a < 128 else tmp ^ 0x1b
  if b == 3:
 return gmul(a, 2) ^ a
  t1=time.time()
 for i in range(100000000):
  mixColumns(0xA3B1BAC6)
t2=time.time()
print(t2-t1)
```

Table 8 shows the time taken for three options for performing a left-shift operation on 100,000,000 random integers, and for the two options listed for the MixColumns representation.

Table 8

Time taken to performs a cyclic shift left and Mixcolumns() transformation of 100,000,000 random 32-bit integers

No.	The representation methods	Time spent (sec)
1.	1st method	403.48764538764954
2.	2nd method	142.70483493804932
3.	3rd method	142.435124874115
4.	MixColumns()	687.4968481063843
5.	MixColumns() with Lut_table	134.1191828250885

The line MixColumns() with Lut_table describes the time taken to display the results of MixColumns using a pre-calculated table.

Table 8 that it is appropriate to use the 3rd method in the Python programming language to perform the cyclic shift operation to the left. The most time was spent on method 1. A little less time was spent in method 3 compared to method 2 due to the or and xor operations. In Table 8 above, you can see that the MixColumns() rendering is faster than the cyclic scroll left rendering when using precomputed tables.

The time taken to encrypt and decrypt 100,000 blocks of plaintext using this software code was compared with other implementations. Table 9 shows the comparison results.

Table 9

The time it takes to encrypt and decrypt 100,000 blocks

No.	Implementation	Time spent (sec) (SM4)	
		Encryption process	Decryption process
1.	Miao X. et al.	36.23312	36.06769
2.	https://github.com/CCWUCMCTS/SM4/blob/main/SM4.py	9.26895	10.14109
3.	https://github.com/windard/sm4/blob/master/Python/sm4.py	6.723578	6.760374
4.	Our method (SM4)	5.526601	5.759675
5.	SM4_Mix	18.53468	18.74289
6.	SM4_Mix (Lut_table)	5.234876	5.482364

From the results in Table 9, we can see that the implementation method proposed in this work has a time-efficient performance compared to other proposed implementation methods.

This work introduces a novel hardware implementation of SM4, termed ultra-low-cost SM4 (ULSM4_2). Similar to UCSM4, the iteration structure of ULSM4 adopts an 8-bit data width as the process unit and facilitates key expansion and encryption computations. The primary innovation lies in the utilization of on-the-fly key expansion and dynamic generation of constant keys through equations on the 8-bit iteration structure of SM4, leading to significant area reduction. A comparison between ULSM4_2 and the latest work UCSM4, based on logic synthesis results,

reveals that ULSM4 occupies merely 2.51K gates at SMIC18 technology, representing an 18.0% reduction compared to UCSM4. These area minimization methods demonstrate their effectiveness, positioning ULSM4 as a more suitable choice for resource-restricted devices.

The iteration structure of ULSM4_2 is illustrated in Figure 4. This architecture is 8-bit, with the exception of the linear substitution, which involves a 32-bit circular shift left and cannot be broken down into byte operations. XR and KR registers function as shift registers, shifting 8 bits to the left per clock cycle. Only the rightmost byte updates through an 8-bit multiplexer controlled by d_s or k_s and is selected for 8-bit XOR operations. Register BR serves as a shift left register, storing the output of the S-Box in the first three cycles of a round and is repurposed to store the lower 24 bits of the linear substitution's output in the last cycle. The output interface is 8-bit, and the results require four cycles to return. For encryption, the round key rk is derived from register KR3, whereas for decryption, it is sourced from register KR0.

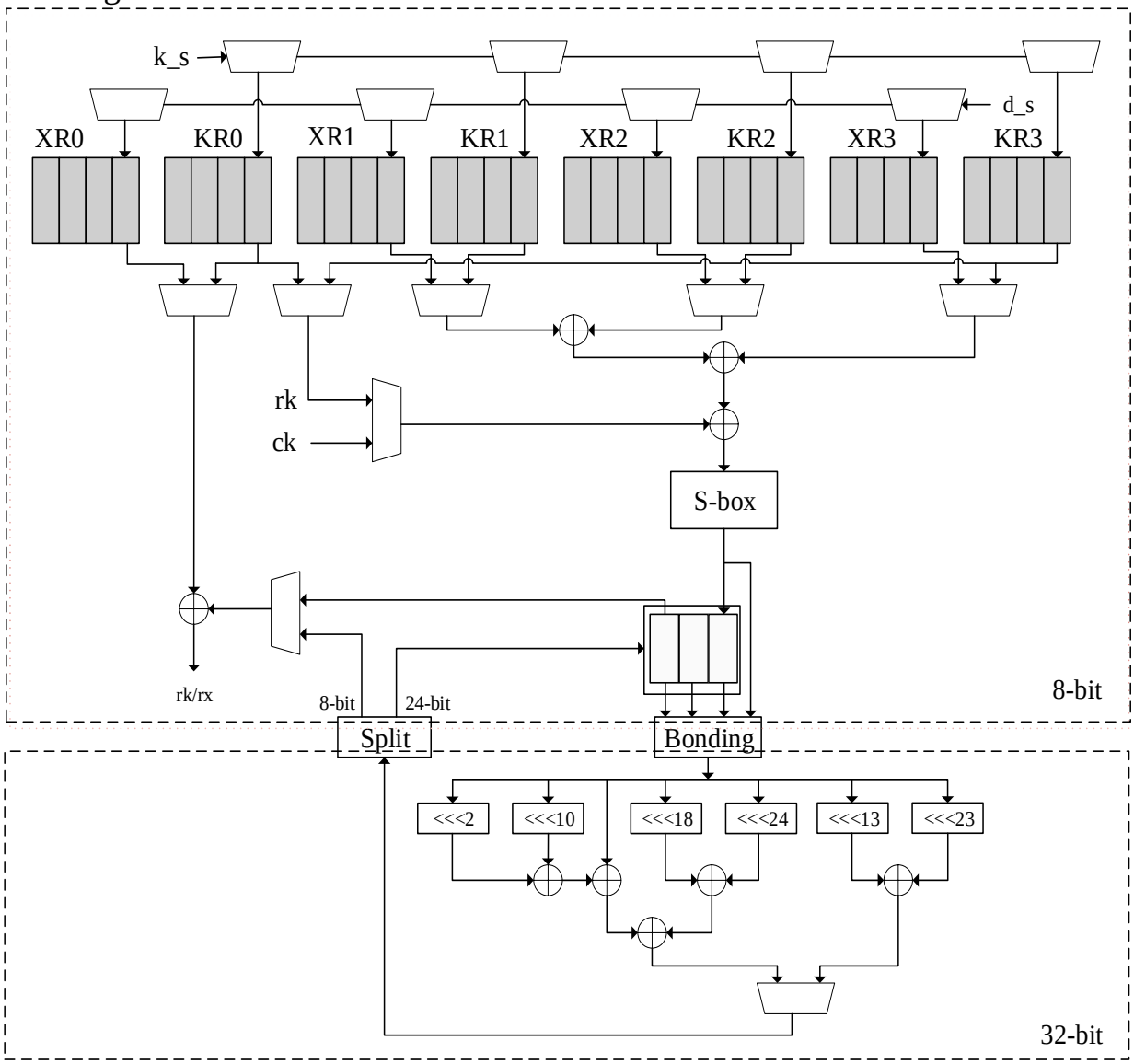


Figure 4. Iteration structure of ULSM4_2

UCSM4_2 features an 8-bit iteration structure with a single S-Box shared for key expansion and encryption. The round keys are pre-computed and stored in memory, and constant keys are implemented using a Look-Up Table (LUT). An additional design, named OTFSM4, is implemented based on UCSM4, applying on-the-fly key expansion. In OTFSM4, constant keys are also implemented using LUT, but they are not rescheduled. Therefore, the key expansion mechanism is the primary distinction between UCSM4_2 and OTFSM4. The synthesis results are presented in Table 10.

Table 10.

Synthesis outcomes for logic @ SMIC18 and 185 MHz

Item	Area/ μm²			Gate count
	Combinational	Non-combinational	Total	
UCSM4 [98]	19,772	10,797	30,569	3060
OTFSM4 [102]	11,794	13,513	25,308	2530
ULSM4 [102]	11,557	13,496	25,053	2510
OTFSM4_2 [this work]	11,744	13,484	25,228	2490
ULSM4_2 [this work]	11,512	13,444	24,956	2470
SM4_Mix	15,494	16,744	32,238	2840
SM4_Mix (with Lut_table)	12,356	14,452	26,808	2560

We also conducted a comparison of ULSM4_2's throughput with UCSM4, SM4_Mix and SM4_Mix (with Lut_table) and the results are presented in Table 11.

Table 11.

Comparison of throughput

Item	Mode	Key	Cycles	Frequency/MHz	Throughput/Mbps
UCSM4 [98]	Encryption	Changed	256	185	92.5
	Decryption	Changed	256	185	92.5
	Encryption	Unchanged	128	185	185
	Decryption	Unchanged	128	185	185
ULSM4 [102]	Encryption	Not care	256	435	217.5
	Decryption	Not care	372	435	149.7
ULSM4_2 [this work]	Encryption	Not care	256	435	225.4
	Decryption	Not care	372	435	162.5
SM4_Mix	Encryption	Not care	288	480	204.5
	Decryption	Not care	404	480	134.7
SM4_Mix (with Lut_table)	Encryption	Not care	256	435	225.4
	Decryption	Not care	372	435	162.5

Throughput is determined by the maximum frequency and the number of cycles required to complete the SM4 algorithm. Since the memory for storing all round keys is on the critical path, the maximum frequency of UCSM4 is constrained to 185 MHz UCSM4 requires 256 cycles to complete encryption or decryption when the input keys are altered and 128 cycles when the input keys remain unchanged. Consequently, the maximum throughput of UCSM4 is 185 MHz

CONCLUSION

The SM4 is evaluated as a linear cryptanalysis method. As a result of the analysis, it was found that $2^{126.4}$ plaintext and ciphertext pairs and $2^{121.7}$ time complexity is required for 23 rounds of the SM4 algorithm for linear cryptanalysis. And to implement the round 23 attack by the multidimensional linear cryptanalysis required N = $2^{122.3}$ plaintext and ciphertext pairs. The time complexity is equivalent to $2^{122.5}$. Notably, our linear approximations emerge as the most effective to date. When MixColumns() transformation is used, it affects only the number of unknowns in the equations in the process of linear cryptanalysis, and does not affect the degree of linearity and their probability.

The SM4 is evaluated as an algebraic cryptanalysis method. As a result of the analysis, it was found that 12519 equations with 2^{36} unknowns for 21 rounds of SM4 algorithm. And solve complexity of system of these equations is equivalent to 2^{108}. In SM4_Mix, the number of unknowns is 2^{64}, and the complexity of the solution is 2^{192}. The number of equations to be formulated in both cases does not differ. The SM4 encryption algorithm is robust to the algebraic cryptanalysis method after round 22.

The SM4 and SM4_Mix encryption algorithms were evaluated using power and differential analysis of a chosen plaintext cryptanalysis method. It was found that the complexity of searching for the encryption key for 4 rounds of the SM4 algorithm is $4 \times 2^4 \times 2^8 = 2^{14}$, and it is $16 \times 2^4 \times 2^8 = 2^{16}$ for the SM4_Mix algorithm.

The methods of implementation of the SM4 encryption algorithm transformations in the Python programming language were studied. And it was found that this implementation method allows to achieve higher efficiency (encryption time for 100,000 blocks is 5.526601 seconds and decryption time is 5.759675 seconds) in terms of time. In the SM4_Mix algorithm, the encryption time for 100,000 blocks is 18.53468 seconds, and the decryption time is 18.74289 seconds. In the SM4_Mix (Lut_table) algorithm, the encryption time for 100,000 blocks is 5.234876 seconds, and the decryption time is 5.482364 seconds.

Determining optimal methods of hardware implementation of the SM4 symmetric block encryption algorithm and its modification variant SM4_Mix. ULSM4_2 exhibits a higher maximum throughput (225.4 Mbps for encryption and 162.5 Mbps for decryption) compared to UCSM4. SM4_Mix (with Lut_table) exhibits a higher maximum throughput (225.4 Mbps for encryption and 162.5 Mbps for decryption) compared to SM4_Mix.

The results obtained in this work can serve as a basis for the development of encryption algorithms, the design of new reflection functions, and the use of cryptanalysis methods.

НАУЧНЫЙ СОВЕТ DSc.03/30.12.2019.FM.01.02
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

LIU LINGYUN

ОЦЕНКА АЛГОРИТМА ШИФРОВАНИЯ SM4 С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ КРИПТОАНАЛИЗА

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

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

Ташкент-2024

Тема диссертации доктора философии (PhD) по физика-математическим наукам зарегестрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2023.4.PhD/FM991.

Диссертация выполнена в Национальном университете Узбекистана имени Мирзо Улугбека.

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

Научный руководитель:	**Абдурахимов Бахтиёр Файзиевич** доктор физика-математических наук, профессор
Официальные оппоненты:	**Кабулов Анвар Василович** доктор технических наук, профессор
	Ние Янг PhD, профессор, Цзининский педагогический университет, Китай
Ведущая организация:	**Термезский государственный университет**

Защиты диссертации состоится "29" августа 2024 года в 1400 часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана. (Адрес: 100174, г.Ташкент, Алмазарский район, ул. Университетская, дом-4. Тел:(+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

С диссертацей можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за №78). (Адрес: 100174, г.Ташкент, Алмазарский район, ул. Университетская, дом-4. Тел:(+99871) 246-02-24).

Автореферат диссертации разослан "16" августа 2024 года.
(протокол рассылки №3 от "24" июнь 2024 года).

М.М. Арипов
Председатель Научного совета по присуждению ученых степеней, д.ф-м.н., профессор

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

А.В. Кабулов
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.т.н., профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии(PhD))

Целью исследования является оценить устойчивость алгоритма симметричного шифрования SM4 и его модификационного варианта SM4_Mix методами криптоанализа и определить оптимальные методы программной и аппаратной реализации.

Объект исследования: алгоритм симметричного шифрования и процессы криптоанализа.

Научная новизна исследования состоит в следующем:

алгоритмы шифрования SM4 и SM4_Mix были оценены с использованием метода линейного криптоанализа и разработаны оптимальные уравнения аппроксимации, необходимые для использования в линейном анализе для 23-раундового алгоритма SM4, который будет использоваться в линейном анализе, $N = 2^{126.4}$ пары открытого текста и зашифрованного текста. были использованы для нападения, необходимость была определена;

в процессе оценки стойкости алгоритма SM4_Mix методом линейного криптоанализа установлено, что количество неизвестных в образуемых уравнениях в 4 раза выше, чем у алгоритма SM4, уровень линейности и их вероятность не различаются, что то есть $2^{-60.5}$ на 20 раундов;

в ходе оценки алгоритмов шифрования SM4 и SM4_Mix методом алгебраического криптоанализа было сформировано 2^{36} алгебраических уравнений сложностью 2^{108} за 21 раунд работы алгоритма SM4, за 21 раунд алгоритма SM4_Mix было сформировано 2^{64} алгебраических уравнения со сложностью решения, равной 2^{192} и доказано, что устойчивость алгоритма к алгебраическому криптоанализу увеличивается при использовании преобразования MixColumns();

в ходе оценки алгоритмов шифрования SM4 и SM4_Mix с использованием метода криптоанализа силового и дифференциального анализа выбранных открытых текстов было установлено, что сложность поиска ключа шифрования в 4 раундах алгоритма SM4 равна 2^{14}, для алгоритма SM4_Mix равна до 2^{16};

определены оптимальные методы реализации L- и S- преобразовании алгоритма SM4, для реализации алгоритмов SM4 и SM4_Mix аппаратно, с высокой пропускной способностью, занимающей меньше места, т.е. 26,808 μm^2, и предложены быстрые и эффективные программные методы, которым требуется 5,234876 секунды для шифрования 100 000 блоков данных и 5,482364 секунды для расшифровки.

Внедрение результатов исследования. Результаты научных исследований по аналитическому и численному моделированию популяционных процессов реализованы в следующих проектах и организациях:

программное обеспечение для оптимальных методов реализации алгоритмов шифрования SM4 и SM4_Mix разработанное в диссертационной работе было экспериментально апробировано в процессе передачи

информации в сети связи и телефонной связи АК «Узбектелеком» Самаркандской городской линии связи («Справка номер 61-03-12/485 от 4 апреля 2024 года Самаркандского филиала «Узбектелеком»). В процессе применения научных результатов предлагаемый программный инструмент оптимальной реализации алгоритма шифрования SM4 позволяет зашифровать 2,21 МБ открытых данных и реверсировать 2,12 МБ зашифрованных данных за 1 секунду, предложенный метод программной реализации программного инструмента алгоритма SM4_Mix и позволил зашифровать 2,33 МБ открытых данных и сбросить 2,22 МБ зашифрованных данных за 1 секунду;

из уравнений оптимальной аппроксимации для алгоритма SM4 23-го раунда, разработанных в диссертационной работе использовано в лабораторных испытаниях для оценки совместимости, точности и эффективности приложений по оценке безопасности коммерческих приложений криптографии, криптографии в сетях и информационных системах во Inner Mongolia Wangxin Information Security Service Co., Ltd (спарвка WXSEC20240315001, 15 марта, 2024) В результате применения научных результатов было установлено, что для проведения атаки линейного криптоанализа на алгоритм SM4 необходимо $2^{126,4}$ пар открытого и зашифрованного текста, а полученные результаты позволили добиться эффективных результатов в процессе оценка устойчивости алгоритма шифрования SM4 к методу линейного криптоанализа;

оптимальные методы программной реализации алгоритма шифрования SM4разработанные в диссертации, в том числе методы оптимальной реализации L- и S-отражений алгоритма SM4, методы реализации отражений алгоритма шифрования SM4 на языке программирования Python, метод описывая S-box как одномерную таблицу, эффективный метод выполнения циклической операции сдвига влево, методы оптимальной реализации алгоритма шифрования на языке программирования Python, что позволило добиться экономии времени по сравнению с другими методами реализации, применен к цифровому научному проекту jsky2021098 «SM4, Исследование алгоритма» были выполнены Школой электронной и информационной инженерии Педагогического университета Цзинин, Цзининский педагогический университет (справка Цзининского педагогического университета № 20240315-001 от 15 марта 2024 г.). В результате применения научных результатов время, затраченное на шифрование 100 000 блоков данных, составило 5,526601 секунды, а время дешифрования – 5,759675 секунды, а предложенные методы реализации позволили повысить производительность алгоритма шифрования SM4.

Структура и объем диссертации. Диссертация состоит из введения, трёх глав, заключения и списка использованной литературы. Объем диссертации составляет 101 страниц.

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

I bo‘lim (I часть; I part)

1. Abdurakhimov B., Abdurazzokov J., Liu Lingyun. Analysis of the use of artificial neural networks in the cryptanalysis of the SM4 block encryption algorithm //AIP Conference Proceedings 2812, 020048 (2023); (№3; Scopus, IF=0.15)

2. Lingyun L., “Wireless Sensor Network-based Acquisition and Analysis of Mechanical Vibration Signals”, International Journal of Mechatronics and Applied Mechanics, Volume 1, Issue 8, 2020. 174-181 p. (№23; Scopus, SJIF=0.17)

3. Ilkhom Rakhmatullaev, Bakhtiyor Abdurakhimov, Liu Lingyun" NewHSA: New Hardware-Implemented Stream Encryption Algorithm" // International Conference on Information Science and Communications Technologies (ICISCT), 2023, pp. 479-484, (№3, Scopus. OAK Rayosatining 29.08.2023 yildagi №01-06/1410/55–son qarori)

4. Abduraximov B., Abdurazzoqov J., Liu Lingyun. “Blokli shifrlash standarti SM4 algoritmida o‘tkazilgan kriptotahlillar natijalari tahlili”, O‘zbekiston Milliy Axborot agentligi UZA ilm-fan bo‘limi// Elektron Jurnal, 2022-yil, oktabr soni, №10(36), 204-212 b. (05.00.00; OAK Rayosatining 2019-yil 28-fevraldagi 262/9.2-son qarori).

5. Lingyun L., “Economic efficiency of software-optimized SM4 algorithm symmetric encryption”, EPRA International Journal of Socio-Economic and Environmental Outlook(SEEO), ISSN: 2455-3662, Volume 10, Issue 9, 2023. -B. 28-32, (№23, https://sjifactor.com/passport.php?id=18322).

6. Lingyun L. “Linear cryptanalysis of the SM4 block cipher algorithm” // Al-Farg‘oniy avlodlari elektron ilmiy jurnali, Toshkent axborot texnologiyalari universiteti Farg‘ona filiali, 2024/1-son, 17-22 b. (05.00.00; OAK Rayosatining 30 sentyabrdagi 343-son qarori).

7. Lingyun L, “Algebraic cryptanalysis of the SM4 symmetric block cipher algorithm”// Electronic Journal of Actual Problems of Modern Science, Education and Training, Urgench State University, ISSN 2181-9750, February, 2024-2, 93-99 p. (01.00.00; №10).

8. Boyquziyev I.M., Allanov O.M., Rakhmatullayev I.R., Lingyun L, “Development of optimal method of hardware implementation of the SM4 and SM4_Mix encryption algorithms // Electronic Journal of Actual Problems of Modern Science, Education and Training, Urgench State University, ISSN 2181-9750, February, 2024-2, 87-93 p. (01.00.00; №10).

II bo‘lim (II часть; II part)

9. Lingyun L., “Research on the Implementation of SM4 National Security Algorithm”, Advances in Higher Education, Singapore, Volume 7, Issue 24, 2023, 224-226 p.

10. Liu Lingyun, “Development of optimal method of hardware implementation of the SM4 and SM4_Mix encryption algorithms”, Ta’limning zamonaviy transformatsiyasi, Konferensiya to‘plami, Volume 6, No. 3, 2024, 113-124 b.

11. Liu Lingyun, “Research on software optimization methods for SM4 and SM4 variant”, “Hisoblash modellari va texnologiyalari” (CMT2024) professor M.I. Isroilov tavalludining 90 yilligiga bag‘ishlangan uchinchi xalqaro seminar to‘plami, 2024, 103-105 b.

12. Liu Lingyun, “Software implementation of SM4 block encryption algorithm in Python programming language”, Proceedings of International Conference on Modern Science and Scientific Studies, April, 19, 2024 in Paris, France. 215-224 p.

13. Liu Lingyun, “Information security protection standards in China: an overview and analysis”, “Zamonaviy informatikaning dolzarb muammolari: o‘tmish tajribasi va istiqbollari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami, Toshkent, 31-may, 2023-yil, 339-340 bet.

14. Abdurakhimov B., Liu Lingyun, “The analysis of modern standard encryption algorithms in the field of information security in China and their importance in data protection”, Abstracts of the international scientific and practical conference “Actual Problems of Mathematical Modeling and Information Technology”, May, 2-3, 2023 in Nukus, Uzbekistan. 169-171 p.

15. Abdurakhimov B., Abdurazzokov J., Liu Lingyun. Analysis of the results of cryptanalysis conducted on the block encryption standard SM4 algorithm, “Science and Technology 2022” сборник статей Международной научно практической конференции июля 2022, Петрозаводск, Россия. 81-87 с.

16. Lingyun L.,Xinzhi W. “Analysis of Conventional Bilateral Band Amplitude and De-adjustment Circuits”, Journal of Jining Normal University, ISSN: 1009-7171, CN 15-1195/G4 Issue 4, 2011. 10-13 p.

17. Lingyun L., Meitao G. “Inhibit Carrier Bilateral Band Analysis”, Digital Technology and Application, ISSN 1007-9416 CN 12-1369/TN, Issue 1, 2013. 194 p.

18. Lingyun L., Pengyu Z. “Low-pass Butterworth Filter Simulation Based on MATLAB”, Digital Technology and Application, ISSN 1007-9416 CN 12-1369/TN, Issue 2, 2013. 124 p.

19. Lingyun L., Dandan D. “Diagnosis and Handling of Faults in Electronic Circuits”, Digital Technology and Application, ISSN 1007-9416 CN 12-1369/TN, Issue 3, 2013. 256 p.

20. Lingyun L., Jianwei H. “The Development and Application of Infrared Wireless Communication”, Inner Mongolia Science Technology and Economy, ISSN 1007-6913 CN 15-1139/N, Issue 3, 2013. 74-76 p.

21. Lingyun L., Meitao G. “The Frontier Outlook of Mobile Communication”, Communication Technology, ISSN 1002-0802 CN 51-1167/TN, Issue 3, 2013. 95-96.100 p.

22. Lingyun L., Jianying C. “The Application of Optical Fiber in Communication”, Inner Mongolia Science Technology and Economy, ISSN 1007-6913 CN 15-1139/N, Issue 5, 2013. 123-125 p.

23. Lingyun L., Meitao G. “Analysis on Single-band”, Communication Technology, ISSN 1002-0802 CN 51-1167/TN, Issue 4, 2013. 128-129.132 p.

24. Abduraximov B., Abdurazzoqov J., Liu Lingyun, “SM4 shifrlash algoritmining barcha raundlari generatsiyasi to‘plamini yaratuvchi dastur”, O‘zbekiston Respublikasi Adliya vazirligining Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi №20.11.2022, DGU 20495.

25. Abduraximov B., Liu Lingyun, “SM4 blokli shifrlash algoritmining optimal amalga oshirilgan dasturiy ta’minoti”, O‘zbekiston Respublikasi Adliya vazirligining Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi №25.03.2023, DGU 35292.

26. Abduraximov B., Liu Lingyun, “SM4_Mix blokli shifrlash algoritmining optimal amalga oshirilgan dasturiy ta’minoti”, O‘zbekiston Respublikasi Adliya vazirligining Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnomasi №25.03.2023, DGU 35293.

Avtoreferat Avtoreferat “O‘zMU xabarlari” jurnali tahririyatida tahrirdan o‘tkazilib, o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 3,5. Adadi 100 dona. Buyurtma № 33/24.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko‘chasi, 83-uy.