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

O‘ZBEKISTON MILLIY UNIVERSITETI

BERDIMURODOV MANSUR ALISHEROVICH

KRIPTOANALIZ MASALALARINI YECHISHNING MANTIQIY USULLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi (fizika-matematika fanlari)

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

Toshkent – 2023

UDK: 004.056.55

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

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

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

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

O‘ZBEKISTON MILLIY UNIVERSITETI

BERDIMURODOV MANSUR ALISHEROVICH

KRIPTOANALIZ MASALALARINI YECHISHNING MANTIQIY USULLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi (fizika-matematika fanlari)

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

Toshkent – 2023

Fizika-matematika fanlari bo‘yicha falsafa doktori (Doctor of Philosophy) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasida №B2020.4.PhD/FM553 raqam bilan ro‘yxatga olingan.

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

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasi (http://ik-fizmat.nuu.uz/) va «ZiyoNet» Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Kabulov Anvar Vasilovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Abduraximov Baxtiyor Fayziyevich** fizika-matematika doktori, professor
	Saidov Abdusobir Abduraxmonovich texnika fanlari doktori, professor
Yetakchi tashkilot:	**“UNICON.UZ” Davlat unitar korxonasi.**

Dissertatsiya himoyasi O‘zbekiston Milliy universiteti huzuridagi DSc.03/30.12.2019.FM.01.02 raqamli Ilmiy kengashning «___»_____2023 yil soat____ dagi majlisida bo‘lib o‘tadi. (Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 227-12-24, faks: (+99871) 246-53-21, 246-02-24, e-mail: nauka@nuu.uz).

Dissertatsiya bilan O‘zbekiston Milliy universitetining Axborot-resurs markazida tanishish mumkin (___ raqami bilan ro‘yxatga olingan). (Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 246-02-24).

Dissertatsiya avtoreferati 2023 yil «____» _____kuni tarqatildi.
(2023 yil «____» _____ dagi _____ raqamli reestr bayonnomasi).

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

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

G.U. Jo‘rayev
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, f.-m.f.d.

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon miqyosida olib borilayotgan ko‘plab ilmiy – amaliy tadqiqotlar natijasida vujudga keladigan kriptografiya va kriptotahlil muammolari aksariyat hollarda shifrlash algoritmlari xossalarini o‘rganish, ularni algebraik ifodalash masalalariga keltiriladi. Shifrlash algoritmi bardoshligini baholash va kriptografik akslantirishlarni ishlab chiqish amaliy matematika, diskret matematika, matematik modellashtirish va ob’ektga yo‘naltirilgan dasturlash kabi sohalardagi tadqiqotlarning ob’ektidir. Kriptotahlil usullari va hisoblash texnikasining rivojlanishi kriptotahlil masalalarini oson yechilishiga va shifrlash algoritmlari bardoshligini pasayishiga asos sifatida xizmat qiladi. Shu sababli, axborot tizimlariga tahdidlarni oshishini hisobga olgan holda, amalda foydalanib kelinayotgan shifrlash algoritmlari ishonchliligini baholash muhim vazifalardan biri bo‘lib qolmoqda.

Hozirgi kunda jahonda kriptografik shifrlash algoritmlarining akslantirishlari hususiyatlarini aniqlash, shifrlash algoritmlarini kriptotahlil usullari yordamida kriptobardoshligini baholash, kriptotahlilning dolzarb masalalaridan biri hisoblanadi. Mazkur holda kriptografik akslantirishlarni algebraik ifodalash, ularning sonli xarakteristikalarini tadqiq qilish muhim ahamiyat kasb etmoqda. Milliy standart sifatida qabul qilingan shifrlash algoritmlari bardoshligini zamonaviy kriptotahlil usullari yordamida baholash va yangi milliy shifrlash algoritmlarini yaratish maqsadli ilmiy tadqiqotlardan hisoblanadi.

Mamlakatimizda fundamental fanlarning ilmiy va amaliy tadbiqiga ega bo‘lgan kriptologiyaning dolzarb yo‘nalishlariga e’tibor ko‘chaytirildi. Jumladan, kriptografik akslantirishlar va algoritmlarni ishlab chiqish sohasida ma’lum yutuqlarga erishilib, axborotlarni uzatish va qayta ishlashning himoyalangan tizimlarini yaratishga alohida e’tibor qaratildi. “Amaliy matematika va matematik modellashtirish” fanlarining ustuvor yo‘nalishlari bo‘yicha xalqaro standartlar darajasida ilmiy tadqiqotlar olib borish asosiy vazifalar va faoliyat yo‘nalishlari etib belgilandi. “Funksional analiz, algebra, differensial tenglamalar, matematik fizika, matematik modellashtirish, hisoblash matematikasi va diskret matematika, ehtimollar nazariyasi va matematik statistika” ustuvor yo‘nalishlar bo‘yicha xalqaro standartlar darajasidagi ilmiy izlanishlar olib borish O‘zR FA V.I.Romanovskiy nomidagi Matematika instituti faoliyatining asosiy vazifalaridan biri hisoblanadi[1]. Qaror ijrosini ta’minlashda algebraik kriptotahlil usullari asosida zamonaviy simmetrik shifrlash algoritmlarining optimal matematik modellarini yaratish va ularning asosida umumiy kriptografik talablarga baholashning mantiqiy usullarini ishlab chiqish va qo‘llash hamda ularning dasturiy ta’minotini yaratish muhim ahamiyatga ega.

O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevraldagi PF-4947 “O‘zbekiston Respublikasini yanada rivojlantrish bo‘yicha harakatlar strategiyasi

[1] O‘zbekiston Respublikasi Prezidentining 2020-yil 7-maydagi “Matematika sohasidagi ta’lim sifatini oshirish va ilmiy- tadqiqotlarni rivojlantirish chora-tadbirlari to‘g‘risida”gi PQ-4708-son qarori.

to‘g‘risida”gi Farmoni, 2017-yil 17-fevraldagi PQ-2789-son “Fanlar akademiyasi faoliyati, ilmiy-tadqiqot ishlarini tashkil etish, boshqarish va moliyalashtirishni yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi, 2017-yil 20-apreldagi PQ-2909-son “Oliy ta’lim tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi va 2018 yil 27 apreldagi PQ-3682 “Innovatsion g‘oyalar, texnologiyalar va loyihalarni amaliyotga joriy qilish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risidagi” qarorlari hamda mazkur faoliyatga tegishli boshqa normativ-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalarni rivojlanishining ustuvor yo‘nalishlariga bog‘liqligi. Dissertatsiya respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Kriptotahlil usullari yordamida baholash masalalari bir qator olimlar, jumladan: Aleks Biryukov, Xovratovich Dmitriy, N.T.Courtois, Nils Fergyuson, Richard Shreppel, Doug Whiting, S.A.Kabakov, O.Ye.Aleksandrov. L.Babenko, M.Aripov, B.Abduraximov, G‘.Tuychiyev, A.Sattarov, D.Kuryazov va boshqalarning ilmiy ishlarida ko‘rib chiqilgan.

Shifrlash algoritmlarini umumiy kriptografik talablar orqali baholashda G‘.Tuychiyev, D.Kuryazov, A.Sattarov, Aleks Biryukov, Xovratovich Dmitriy va boshqalarning ishlarida shuningdek AES, GOST R34.12-2015 (Kuznechik) standart shifrlash algoritmlariga nisbatan algebraik kriptotahlil usuli N.T.Courtois, Aleks Biryukov, Xovratovich Dmitriy va boshqalarning ishlarida samarali natijalar olingan.

Shifrlash algoritmi va bardoshli kriptografik akslantirishlarni baholash masalalari bilan bog‘liq tadqiqotlar bir qator olimlar tomonidan tadqiq qilingan, jumladan: A.Youssef, N.Courtois, B.Shnayer, K.Shennon, G.Murtaza, I.Hussain, J.Nakahara, J.Rijmen, K.Chand, K.Gupta, K.Nyberg, M.Malik, Hasan Omar, Zhou Yuyang, P.Junod, M.Aripov, M.Karimov, B.Abduraximov, R.Oleynikov, T.Chalkin, G.U.Jo‘rayev, D.Kuryazov, A.Sattarov, A.V.Kabulov va boshqalar.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti O‘zbekiston Milliy universitetining ilmiy-tadqiqot ishlari rejalariga muvofiq, BV-M-F4-004 “Funksional jadvallar algebrasi asosida murakkab tizimlar boshqarishini algoritmlashtirish prinsiplarini ishlab chiqish” va F3-201906117 “Orolbo‘yi qishloq xo‘jaligi ishlab chiqarishida ekologik vaziyatlar ta’sirini aniqlash monitoringini yuritishning dasturiy ta’minoti” ilmiy-tadqiqot loyihalari doirasida bajarilgan.

Tadqiqotning maqsadi AES va GOST R34.12-2015(Kuznechik) kriptografik shifrlash algoritmlaridagi akslantirishlarni va ularning bardoshligini tahlil qilish, algebraik kriptotahlil usuli yordamida baholash hamda mantiqiy usullar yordamida turli bazislardagi matematik modelini yaratish va

murakkabligini baholashdan iborat.

Tadqiqotning vazifalari:

algebraik kriptotahlil usullari asosida zamonaviy simmetrik shifrlash algoritmlarining optimallashtirilgan matematik modellarini yaratish;

zamonaviy simmetrik shifrlash algoritmlarining yaratilgan matematik modellari asosida umumiy kriptografik talablarga baholashning mantiqiy usullarini ishlab chiqish;

zamonaviy simmetrik shifrlash algoritmlarining matematik modellari asosida turli bazislardagi tenglamalar tizimini yaratish va yechish algoritmlarini ishlab chiqish hamda ularning murakkabligini baholash;

AES va GOST R34.12-2015 (Kuznechik) simmetrik blokli shifrlash algoritmlaridagi akslantirishlarni turli bazisdagi bul funksiyalarga keltirish mezonlari va algoritmini ishlab chiqish;

AES-128 va GOST R34.12-2015 (Kuznechik) standartidagi akslantirishlarning, Jegalkin ko‘phadidagi va dizyunktiv normal shakldagi bul tenglamalar tizimini yechishning dasturiy ta’minotini ishlab chiqish;

Kuznechik shifrlash algoritmi mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishda optimallashtirilgan bul formulalarida ifodalash;

bul monoton funksiyalarning maksimal yuqori nolini izlash asosida mantiqiy tenglamalar tizimlarining maksimal qism tizimini topish va mantiqiy tenglamalar tizimlarini yechish algoritmi ishlab chiqish;

ishlab chiqilgan optimallashtirilgan matematik modellar asosida algebraik kriptotahlilni o‘tkazish.

Tadqiqotning ob’ekti kriptografik algoritmlar, akslantirishning matematik modellari, bul tenglamalar tizimi, algoritmlar mikrobuyruqlarining bul funksiya shakllaridan iborat.

Tadqiqotning predmeti akslantirishning matematik modellari, kriptografik algoritmlar kriptobardoshligi, algebraik va mantiqiy jarayonlar, kriptoanaliz tahlili va tadqiqi, kriptotizimlarning bul jadvallari va kriptografik algoritmlarning bul funksiyalari, kriptoalgoritmlar mikrobuyruqlari.

Tadqiqotning usullari. Tadqiqot ishida kriptotahlil, bul tenglamalar nazariyasi, mikrobuyruqlar nazariyasi, mantiqiy modellar, algebra va matematik mantiq usullari va ob’ektga yo‘naltirilgan dasturlash usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

AES, GOST R34.12-2015 (Kuznechik), A5/1 algoritmlarining algebraik kriptotahlil usullari asosida optimallashtirilgan matematik modellari yaratilgan;

AES, GOST R34.12-2015 (Kuznechik) zamonaviy simmetrik shifrlash algoritmlari qurilgan matematik modellari asosida umumiy kriptografik talablarga baholangan va ularga nisbatan turli bazisda algebraik kriptotahlil o‘tkazilgan;

Kuznechik shifrlash algoritmi mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishda optimallashtirilgan bul formulalari yaratilgan;

AES, GOST R34.12-2015 (Kuznechik) va A5/1 simmetrik shifrlash algoritmlaridagi akslantirishlarni turli bazisdagi bul funksiyalarga keltirish

mezonlari va algoritmi ishlab chiqilgan hamda bir bazisdan ikkinchi bazisga transformatsiya qilish teoremalari isbotlangan;

Bul monoton funksiyalarning maksimal yuqori nolini izlash asosida mantiqiy tenglamalar tizimlarini yechish algoritmlari ishlab chiqilgan va ularning murakkabligi baholangan.

Tadqiqotning amaliy natijalari quyidagilardan iborat**:**

Kriptotizimlardagi algoritmlarning graf-sxemasi asosida bul jadvallari qurilgan;

Kuznechik shifrlash algoritmlari mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishda optimallashtirilgan bul formulalari yaratilgan;

AES-128 va GOST R34.12-2015 (Kuznechik) standartlaridagi akslantirishlarning optimallashtirilgan matematik modellari ishlab chiqilgan;

AES-128 va GOST R34.12-2015(Kuznechik) standartlari turli bazisdagi matematik modellar asosida algebraik kriptotahlil o‘tkazilgan va kriptobardoshligi baholangan;

shifrlash algoritmlaridagi akslantirishlarning bul funksiyalarga asoslangan matematik modeli qurilgan;

Jegalkin ko‘phadidagi va dizyunktiv normal shakldagi chiziqsiz bul tenglamalar tizimini yechishning dasturiy ta’minoti ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi matematik mulohazalarning qat’iyligi, diskret matematika va matematik mantiq usullarini qo‘llanilganligi, zamonaviy simmetrik shifrlash algoritmlarining matematik modellari yaratilganligi, umumiy kriptografik talablarga baholashning mantiqiy usullarini ishlab chiqilganligi bilan asoslangan.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati zamonaviy simmetrik shifrlash algoritmlarining ishlab chiqilgan va optimallashtirilgan matematik modellari asosida umumiy kriptografik talablarga baholashning mantiqiy usullarini ishlab chiqilganligi va bu modellar asosida algebraik kriptotahlil olib borilganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati o‘rnatilgan mikroprotsessorli tizimlarda Kuznechik shifrlash algoritmi mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishda optimallashtirilgan bul formulalari yaratilgan va ularni apparat-dasturiy vositalarda qo‘llanishga qulayligi asoslangan.

Tadqiqot natijalarining joriy qilinishi. AES, Kuznechik, A5/1 zamonaviy shifrlash algoritmlari uchun yaratilgan va optimallashtirilgan matematik modellar va umumiy kriptografik talablarga baholashda olingan natijalar asosida:

AES, Kuznechik shifrlash algoritmlarining optimallashtirilgan matematik modeli hamda umumiy kriptografik talablarga baholash natijalari OT-Atex-2018-486 “Mantiqiy boshqaruv va axborot xavfsizligi tizimlarini dasturlashtirilgan mantiqiy kontrollerlar va ularni loyihalovchi avtomatlashtirilgan CAD mantiqiy tizimi asosida amalga oshirish” loyihasida shifrlash algoritmlarini mikrokontrollerlarga yozishda mikrobuyruqlarning bul funksiya shakllarini tahlil qilish va optimallashtirishda foydalanilgan (Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti 2022-yil 17-maydagi 04/10-2807–son

ma’lumotnomasi). Ilmiy natijalarni qo‘llash mikrokontrollerga shifrlash algoritmlarini optimal yozish va tahlil qilish imkonini bergan.

zamonaviy simmetrik shifrlash algoritmlari uchun shifrlash algoritmlarini umumiy kriptografik talablarga baholash qoidalaridan “UNICON.UZ” DUKda olib borilayotgan “Kriptografik algoritmlar yaratish” loyihasi doirasida kriptografik algoritmlarni zamonaviy kriptotahlil usullari yordamida baholash jarayonida foydalanilgan. Shuningdek dissertatsiya ishida keltirilgan GOST R34.12-2015 simmetrik blokli shifrlash algoritmidagi akslantirishlarni turli bazisdagi bul funksiyalarga keltirish mezonlari va algoritmini qo‘llash yechimlaridan “UNICON.UZ” DUKda milliy himoyalangan tizimlarda foydalanilayotgan simmetrik blokli shifrlash algoritmlari bardoshligini baholashda qo‘llanilgan (“UNICON.UZ” DUKning 2022-yil 10-iyundagi 5-3/945–son ma’lumotnomasi). Ilmiy natijalarni qo‘llash milliy himoyalangan tizimlarda foydalanilayotgan simmetrik blokli shifrlash algoritmlari bardoshligini baholash va tahlil qilish imkonini bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 10 ta ilmiy-amaliy anjumanlarda, jumladan 6 ta xalqaro va 4 ta respublika miqyosidagi ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha 18 ta ilmiy ish chop etilgan, shulardan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining falsafa doktori dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarda 8 ta maqola, jumladan 4 tasi xorijiy (4 ta skopus) va 5 tasi Respublika jurnallarida chop etilgan. Shuningdek, 4 ta EHM uchun yaratilgan dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish qismi, uchta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovadan tashkil topgan. Dissertatsiyaning hajmi 114 betni tashkil etgan.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi, tadqiqot maqsadi va vazifalari, tadqiqot ob’ekti va predmeti tavsiflanadi, tadqiqotning respublikada fan va texnologiyalarni rivojlanishining ustuvor yo‘nalishlariga muvofiqligi ko‘rsatiladi. Izlanishning ilmiy yangiligi va amaliy natijalari aniqlangan, olingan natijalarning ishonchliligi asoslangan, olingan natijalarning ilmiy-amaliy ahamiyati ko‘rsatilgan. Natijalar, ularni amaliyotga tatbiq etish, nashr etilgan ishlar va dissertatsiya tuzilishi to‘g‘risida ma’lumotlar berilgan.

Dissertatsiyaninig **“Zamonaviy simmetrik shifrlash algoritmlarining algebraik kriptotahlil uchun optimallashtirilgan matematik modellarini yaratish va umumiy kriptografik talablarga baholash”** nomli I bobida AES shifrlash algoritmining *SubBytes*, *ShiftRows*, *MixColumns* va *AddRoundKey* akslantirishlari, GOST R34.12-2015(Kuznechik) standart algoritmidagi *S, L, X* akslantirishlarining bul funksiyalarga asoslangan matematik modelini qurish algoritmi va har bir akslantirishlarning Jegalkin ko‘phadi hamda dizyunktiv

normal shakllaridagi(d.n.sh.) matematik modeli keltirilgan. Bul funksiyalar asosida akslantirishlarni umumiy kriptografik talablarga baholash tahlil qilingan. 1.1-paragrafda algebraik kriptotahlil asosida shifrlash algoritmlarini umumiy kriptografik talablarga baholash keltirilgan. Bul funksiya va akslantirishlarni baholash uchun zarur bo‘lgan ayrim matematik tushunchalar keltirilgan. 1.2-paragrafda AES kriptografik algoritmining optimallashtirilgan matematik modellarini yaratish va umumiy kriptografik talablarga baholash keltirilgan. Shuningdek, ushbu paragrafda shifrlash algoritmidagi har bir akslantirishlarning bul funksiyalarga asoslangan matematik modellari qurilgan. *AddRoundKey* akslantirishi raund kalitini qo‘shish akslantirishi bo‘lib, akslantirishga kiruvchi va chiquvchi bitlar quyidagicha aniqlangan $y_j = x_j \oplus k_{i\,j}, (j = \overline{0,127})$ (bu yerda $K_i = (k_{i0}, k_{i1}, \cdots, k_{i127}), (i = \overline{0,10})$ raund kalitlar). *SubBytes* chiziqsiz akslantirishi a_i kiruvchi va b_i chiquvchi bitlari mos ravishda 256 ta turli qiymat qabul qilishi mumkin. Kiruvchi a_i bayt qiymatlarini o‘sish tartibida unga mos ravishda chiquvchi b_i bayt qiymatlari 8 o‘zgaruvchili 8 ta bul funksiyasining rostlik jadvali hosil bo‘ladi. Bu yerda $i = 8 \cdot t,\ \ t = \overline{0,15}$ *SubBytes* chiziqsiz akslantirishidagi chiquvchi $b_i (i = \overline{0,15})$ bayt quyidagicha aniqlanadi:

$$\left.\begin{array}{l} y_{i*8} = S_0(a_i), y_{i*8+1} = S_1(a_i), \cdots, y_{i*8+7} = S_7(a_i) \\ b_i = y_{i*8} \,||\, y_{i*8+1} \,||\, y_{i*8+2} \,||\, y_{i*8+3} \,||\, y_{i*8+4} \,||\, y_{i*8+5} \,||\, y_{i*8+6} \,||\, y_{i8+7} \end{array}\right\} \quad (1)$$

Aniqlangan $S_i(x)$, chiquvchi bit funksiyalarning qiymati asosida mukammal d.n.sh. va undan so‘ng Karto – Karno va Kvayn minimallashtirish usullari yorda-mida minimal d.n.sh. ifodasiga olib kelingan. AES shifrlash algoritmidagi *SubBytes* va *SubBytes teskari* chiziqsiz akslantirishlaridan chiquvchi y_i $(i = \overline{0,7})$ bitlarning minimal d.n.sh. va algebraik normal shakldagi(a.n.sh.) optimallashtirilgan matematik modellari qurilgan. *SubBytes* va *SubBytes teskari* chiziqsiz akslantirishlarini ifodalovchi bul funksiyalar umumiy kriptografik talablarga baholandi. *SubBytes* chiziqsiz akslantirishini ifodalovchi bul funksiyaning umumiy kriptografik talablarga baholari 1-jadvalda keltirib o‘tilgan.

SubBytes akslantirish $(i = 8 \cdot t,\ t = \overline{0,15})$ 1-jadval.

SubBytes	y_i	y_{i+1}	y_{i+2}	y_{i+3}	y_{i+4}	y_{i+5}	y_{i+6}	y_{i+7}
Balanslanganlik	+	+	+	+	+	+	+	+
Regulyarlik	+							
A.n.sh.da algebraik chiziqsizlik ($def(y)$)	7	7	7	7	7	7	7	7
Chiziqsizlik $N(y)$	112	112	112	112	112	112	112	112
Algebraik immuniteti	2							
Korrelyatsion immunitet	0	0	0	0	0	0	0	0
A.n.sh. da e.k. soni	108	110	112	129	134	143	131	130

D.n.sh. da algebraik chiziqsizlik ($def(y)$)	7	8	7	7	8	7	7	7
D.n.sh.da e.k. soni	55	52	59	49	54	50	53	49

ShiftRows(SR) – bu baytli siljitish akslantirishi bo‘lib, akslantirishning bitlar shaklidagi ifodasi quyidagi (2) kabi aniqlanadi.

$$\left.\begin{array}{l} y_k = x_k; y_{8+k} = x_{40+k}; y_{16+k} = x_{80+k}; y_{24+k} = x_{120+k}; y_{32+k} = x_{32+k}; y_{40+k} = x_{72+k}; \\ y_{48+k} = x_{112+k}; y_{56+k} = x_{24+k}; y_{64+k} = x_{64+k}; y_{72+k} = x_{104+k}; y_{80+k} = x_{16+k}; y_{88+k} = x_{56+k}; \\ y_{96+k} = x_{96+k}; y_{104+k} = x_{8+k}; y_{112+k} = x_{48+k}; y_{120} = x_{88+k}; \text{ bu yerda } k = \overline{0,7} \end{array}\right\} (2)$$

MixColums(MC) akslantirishdan chiquvchi $b_j\ (j = \overline{0,15})$ baytlarni bul funksiyaga o‘tkazish uchun (3) tengliklardan foydalanish mumkin.

$$\left.\begin{array}{l} f(x) = (t_7t_6t_5t_4t_3t_2t_1t_0); \quad 0\bullet f(x) = 0; \quad 01\bullet f(x) = f(x); \\ 02\bullet f(x) = x\bullet f(x) = \begin{cases} (t_6t_5t_4t_3t_2t_1t_0 0) \text{ agar } t_7 = 0 \\ (t_6t_5t_4t_3t_2t_1t_0 0) \oplus (00011011) \text{ agar } t_7 = 1 \end{cases} \\ 03\bullet f(x) = \{01 \oplus 10\}\bullet f(x) = \{01_2 \bullet f(x)\} \oplus \{10_2 \bullet f(x)\} = f(x) \oplus x\bullet f(x) \end{array}\right\} \quad (3)$$

Akslantirishdan chiquvchi $y_j\ (j = \overline{0,127})$ bitlarning bul funksiya shaklidagi matematik modellari yordamida(14-ilova) 1-2 tasdiqlar isbotlangan.

1-tasdiq. *MixColumns* chiziqli akslantirishdan chiquvchi har bir bitning, kiruvchi nechta bit qiymatlarga bog‘liqlik qiymati mos ravishda {5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5} qiymatlarga teng.

2-tasdiq. *MixColumns* chiziqli akslantirishga kiruvchi har bir bitning chiquvchi nechta bit qiymatlarga bog‘liqlik qiymati mos ravishda {11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5} qiymatlarga teng.

1.3-paragrafda GOST R34.12-2015 standart kriptografik algoritmining optimallashtirilgan matematik modellarini yaratish va umumiy kriptografik talablarga baholash keltirilgan. Kuznechik kriptografik algoritmining kalitlarni (*X*(*K*,*M*)) qo‘shish algoritmi quyidagi (4) formula bilan amalga oshiriladi:

$$\left.\begin{array}{l} X(K_i, M) = K_i \oplus M; (i = \overline{1,10}) M = (m_0 \| m_1 \| ... \| m_{127}); \\ K_i = (k_0 \| k_1 \| ... \| k_{127}); \ X = (k_0 \| k_1 \| ... \| k_{127}) \oplus (m_0 \| m_1 \| ... \| m_{126} \| m_{127}) \end{array}\right\} \quad (4)$$

S–chiziqsiz akslantirishdan chiquvchi $y_i\ (i = \overline{0,127})$ bitlarning (a,b,c,d,e,f,g,h) 8 o‘zgaruvchili bul funksiya shakldagi matematik modeli

qurilgan. S va S^{-1} chiziqsiz akslantirishlarini ifodalovchi bul funksiyalar umumiy kriptografik talablarga baholandi. S akslantirishining kriptografik talablarga bahosi 2-jadvalda keltirilgan.

S chiziqsiz akslantirish $(i = 8 \cdot t,\ t = \overline{0,15})$ 2-jadval.

S	y_i	y_{i+1}	y_{i+2}	y_{i+3}	y_{i+4}	y_{i+5}	y_{i+6}	y_{i+7}
Balanslanganlik	+	+	+	+	+	+	+	+
Regulyarlik	+							
A.n.sh.da algebraik chiziqsizlik ($def(y)$)	7	7	7	7	7	7	7	7
Chiziqsizlik $N(y)$	104	106	116	104	110	106	102	104
Algebraik immuniteti	3							
Korrelyatsion immunitet	0	0	0	0	0	0	0	0
A.n.sh. da e.k. soni	137	132	143	135	122	125	123	122
D.n.sh. da algebraik chiziqsizlik ($def(y)$)	7	7	7	7	7	8	7	7
D.n.sh.da e.k. soni	53	50	49	49	62	55	52	48

L chiziqli akslantirishning umumiy matematik modellari (13-ilova) asosida 3,4-tasdiqlar isbot qilingan.

3-tasdiq. L chiziqli akslantirishdan chiquvchi har bir bitning, kiruvchi nechta bit qiymatlarga bog‘liqlik qiymati mos ravishda {98, 100, 87, 82, 88, 97, 97, 93, 100, 91, 103, 104, 92, 87, 99, 107, 102, 99, 91, 102, 101, 96, 103, 87, 101, 96, 106, 96, 102, 96, 90, 101, 106, 95, 88, 97, 91, 90, 100, 102, 103, 97, 101, 96, 92, 94, 90, 100, 106, 102, 103, 101, 94, 106, 100, 106, 93, 96, 96, 90, 95, 97, 93, 87, 99, 107, 102, 101, 106, 104, 106, 99, 105, 102, 102, 100, 106, 104, 101, 106, 102, 103, 87, 100, 99, 95, 99, 108, 106, 95, 91, 103, 99, 97, 95, 101, 105, 98, 93, 99, 94, 92, 101, 91, 98, 95, 98, 94, 91, 93, 97, 101, 99, 99, 88, 85, 82, 94, 87, 93, 65, 62, 40, 42, 44, 54, 57, 59} qiymatlarga teng.

4-tasdiq. L chiziqli akslantirishga kiruvchi har bir bitning chiquvchi nechta bit qiymatlarga bog‘liqlik qiymati mos ravishda {123, 101, 106, 89, 103, 97, 108, 94, 105, 107, 98, 95, 105, 68, 87, 77, 106, 102, 95, 103, 93, 90, 100, 81, 109, 80, 90, 107, 77, 86, 94, 69, 109, 99, 108, 105, 108, 104, 106, 95, 102, 103, 104, 107, 105, 83, 103, 88, 93, 97, 77, 75, 100, 91, 89, 95, 118, 109, 100, 104, 104, 100, 91, 110, 77, 74, 80, 76, 83, 88, 94, 94, 114, 111, 107, 105, 108, 86, 103, 95, 114, 103, 115, 112, 112, 90, 101, 97, 116, 77, 83, 116, 72, 74, 64, 78, 114, 93, 99, 107, 95, 101, 98, 81, 114, 118, 76, 99, 115, 62, 86, 65, 123, 79, 83, 93, 101, 86, 115, 93, 70, 56, 71, 75, 80, 60, 83, 84} qiymatlarga teng.

Kuznechik shifrlash algoritmining umumiy analitik shakli aniqlangan. Aniqlangan analitik shaklda quyidagicha noma’lumlar va tenglamalar hosil bo‘ldi (3-jadval).

Kuznechik algoritmi umumiy parametrlari 3-jadval.

Raund	Kalit noma'lum	Jami noma'lum	$def(y)$	E.k. soni a.n.sh.da	E.k. soni d.n.sh.da
1	128	$2\cdot128$	7	$143\cdot107$	$\le r_1 = 2^8\cdot62\cdot2^{106}+1$
2	$2\cdot128$	$3\cdot128$	49	$(143\cdot107)^2\cdot107$	$\le r_2 = r_1^8\cdot62\cdot2^{106}+1$
n	$128\cdot n$	$(n+1)\cdot128$	7^n	$(143\cdot107)^7\cdot107$	$\le r_n = r_{n-1}^{\ 8}\cdot62\cdot2^{106}+1$
10	$10\cdot128$	$11\cdot128$	1408	$(143\cdot107)^{10}\cdot107$	$\le r_{10} = r_9$
Jami	1280	1408	1408	$\approx 7.53\cdot10^{43}$	

1.4-paragrafda A5/1 oqimli shifrlash algoritmining turli bazisdagi matematik modellarini qurish keltirilgan. Har bir kalit bitini hisoblash qadamida $m = maj(x_8, y_{10}, z_{10})$ major qiymat hisoblanadi. Major qiymatni aniqlash algoritmining $\{\vee,\wedge,\neg\}$ va $\{\oplus,\wedge,1\}$ bazislarida bul funksiyaga asoslangan matematik modellari taklif qilingan: $m = x_8y_{10} \vee x_8z_{10} \vee y_{10}z_{10}$; $m = x_8y_{10} \oplus x_8z_{10} \oplus y_{10}z_{10}$.

***X* registrida siljish.** X registrida x_8 bit qiymatining major qiymatiga teng bo'lish yoki bo'lmasligidan qat'iy nazar siljitish jarayonini $\{\oplus,\wedge,1\}$ bazisi Jegalkin ko'phadidagi matematik modeli (5), $\{\vee,\wedge,\neg\}$ bazisi d.n.sh.dagi matematik modeli (6) ko'rinishida aniqlangan:

$$\left.\begin{aligned} &t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18};\\ &x_i = (m \leftrightarrow x_8)x_{i-1} \vee \overline{(m \leftrightarrow x_8)}x_i = x_{i-1} \oplus x_8x_i \oplus x_8x_{i-1} \oplus mx_i \oplus mx_{i-1};\\ &(\text{bu yerda } i = \overline{18,1});\ x_0 = t \oplus x_8x_0 \oplus x_8t \oplus mx_0 \oplus mt. \end{aligned}\right\} \quad (5)$$

$$\left.\begin{aligned} &t = x_{13}x_{16}x_{17}\overline{x_{18}} \vee x_{13}\overline{x_{16}x_{17}x_{18}} \vee x_{13}x_{16}\overline{x_{17}}x_{18} \vee x_{13}\overline{x_{16}}x_{17}x_{18} \vee\\ &\vee\overline{x_{13}}x_{16}\overline{x_{17}x_{18}} \vee \overline{x_{13}}x_{16}x_{17}x_{18} \vee \overline{x_{13}x_{16}}x_{17}\overline{x_{18}} \vee \overline{x_{13}x_{16}x_{17}}x_{18}\\ &x_i = (m \leftrightarrow x_8)x_{i-1} \vee \overline{(m \leftrightarrow x_8)}x_i = x_i\,x_{i-1} \vee mx_8x_{i-1} \vee m\overline{x_8}x_i \vee\\ &\vee\overline{m}x_8x_i \vee \overline{m}\,\overline{x_8}x_{i-1}; \qquad (\text{bu yerda } i = \overline{18,1})\\ &x_0 = (m \leftrightarrow x_8)t \vee \overline{(m \leftrightarrow x_8)}x_0 = x_0t \vee mx_8t \vee m\overline{x_8}x_0 \vee \overline{m}x_8x_0 \vee \overline{m}\,\overline{x_8}t. \end{aligned}\right\} \quad (6)$$

***Y* registrida siljish.** Y registrida siljitish jarayonini $\{\oplus,\wedge,1\}$ bazisi Jegalkin ko'phadidagi matematik modeli (7), $\{\vee,\wedge,\neg\}$ bazisi d.n.sh. formulasidagi optimallashtirilgan matematik modeli (8) ko'rinishida aniqlangan:

$$\left.\begin{aligned} &t = y_{20} \oplus y_{21}; \quad (\text{bu yerda } i = \overline{21,1});\\ &y_i = (m \leftrightarrow y_{10})y_{i-1} \vee \overline{(m \leftrightarrow y_{10})}y_i = y_{i-1} \oplus y_{10}y_i \oplus y_{10}y_{i-1} \oplus my_i \oplus my_{i-1};\\ &y_0 = (m \leftrightarrow y_{10})t \vee \overline{(m \leftrightarrow y_{10})}y_0 = mt \oplus y_{10}t \oplus my_0 \oplus y_{10}y_0 \oplus t. \end{aligned}\right\} \quad (7)$$

$$\left.\begin{array}{l} t = y_{20} \oplus y_{21} = y_{20}\overline{y_{21}} \vee \overline{y_{20}}y_{21};\ \ y_i = (m \leftrightarrow y_{10})y_{i-1} \vee \overline{(m \leftrightarrow y_{10})}y_i = y_i\, y_{i-1} \vee \\ \vee my_{10}y_{i-1} \vee m\overline{y_{10}}y_i \vee \overline{m}y_{10}y_i \vee \overline{m}\,\overline{y_{10}}y_{i-1};\quad (\text{bu yerda } i = \overline{21,1}); \\ y_0 = (m \leftrightarrow y_{10})t \vee \overline{(m \leftrightarrow y_{10})}y_0 = y_0 t \vee my_{10}t \vee m\overline{y_{10}}y_0 \vee \overline{m}y_{10}y_0 \vee \overline{m}\,\overline{y_{10}}t. \end{array}\right\} \quad (8)$$

***Z* registrida siljish.** Z registrida siljitish jarayonini $\{\oplus, \wedge, 1\}$ bazisi Jegalkin ko‘phadidagi matematik modeli (9), $\{\vee, \wedge, \neg\}$ bazisi d.n.sh. formulasidagi optimallashtirilgan matematik modeli (10) ko‘rinishida aniqlangan:

$$\left.\begin{array}{l} t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22};\ \ z_i = (m \leftrightarrow z_{10})z_{i-1} \vee \overline{(m \leftrightarrow z_{10})}z_i = \\ = z_{i-1} \oplus z_{10}z_i \oplus z_{10}z_{i-1} \oplus mz_i \oplus mz_{i-1}; \qquad \left(\text{bu yerda } i = \overline{22,1}\right) \\ z_0 = (m \leftrightarrow z_{10})t \vee \overline{(m \leftrightarrow z_{10})}z_0 = mt \oplus z_{10}t \oplus mz_0 \oplus z_{10}z_0 \oplus t. \end{array}\right\} \quad (9)$$

$$\left.\begin{array}{l} t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22} = z_7 z_{20} z_{21}\overline{z_{22}} \vee z_7\overline{z_{20}}\,\overline{z_{21}}\,\overline{z_{22}} \vee z_7 z_{20}\overline{z_{21}}z_{22} \vee z_7\overline{z_{20}}z_{21}z_{22} \vee \\ \vee \overline{z_7}z_{20}\,\overline{z_{21}}\,\overline{z_{22}} \vee \overline{z_7}z_{20}z_{21}z_{22} \vee \overline{z_7}\,\overline{z_{20}}z_{21}\overline{z_{22}} \vee \overline{z_7}\,\overline{z_{20}}\,\overline{z_{21}}z_{22};\ \ z_i = (m \leftrightarrow z_{10})z_{i-1} \vee \\ \vee \overline{(m \leftrightarrow z_{10})}z_i = z_i\, z_{i-1} \vee mz_{10}z_{i-1} \vee m\overline{z_{10}}z_i \vee \overline{m}z_{10}z_i \vee \overline{m}\,\overline{z_{10}}z_{i-1}; (\text{bu yerda } i = \overline{22,1}) \\ z_0 = (m \leftrightarrow z_{10})t \vee \overline{(m \leftrightarrow z_{10})}z_0 = z_0 t \vee mz_{10}t \vee m\overline{z_{10}}z_0 \vee \overline{m}z_{10}z_0 \vee \overline{m}\,\overline{z_{10}}t. \end{array}\right\} \quad (10)$$

Dissertatsiyaning II bobida mantiq algebrasida monoton funksiyalarning maksimal yuqori nolini topish asosida bul tenglamalar tizimining maksimal qism tizimlari topish va yechish uchun algoritm taklif qilingan. Shuningdek bobda dizyunktiv normal shakllar sinfidagi mantiqiy funksiyalarni minimallashtirishda analitik o‘zgarishlar, mantiqiy ifodalarni umumiy shaklga aylantirish uchun ba’zi analitik formulalar keltirilgan. Turli xil analitik ifodalarni hosil qilish va transformatsiya masalalari yechilgan va mantiq algebrasi funksiyalarining bir bazisdan ikkinchi bazisga transformatsiya qilish teoremalari isbotlangan. Hamda Jegalkin ko‘phadini optimaltirish usullari keltirib o‘tilgan.

2.1-paragrafda monoton mantiqiy bul funksiyalarining maksimal yuqori nolini topish usuli asosida mantiqiy bul tenglamalar tizimining(TT) maksimal qism tizimlarini topish masalasini yechilgan. Ushbu paragrafda monoton mantiqiy funksiyalarning maksimal yuqori nollarni qidirish masalasining A_K Katerinochkina algoritmining samarali A_M modifikatsiyasi ishlab chiqilgan.

Mantiqiy bul tenglamalar tizimining maksimal qism tizimlarini topish masalasini yechish

$$M = \left\{ f_1(x_1, x_2, ..., x_n) = 1;\ f_2(x_1, x_2, ..., x_n) = 1;\ \ldots;\ f_m(x_1, x_2, ..., x_n) = 1. \right\} \quad (11)$$

(11) kabi mantiqiy tenglamalar tizimi berilgan bo‘lsin. Tizimning maksimal qism tizimlarini topish algoritmi quyidagi bosqichlarni o‘z ichiga oladi: 1) ifodalarning qiymatlar tasvirini hisoblash; 2) yuqoridagi algoritmidan foydalangan holda maksimal qism tizimlarni shakllantirish. Har bir (12) qism tizimlarning mosligini tahlil qilish.

$$\left\{ f_{j_1}(x_1, ..., x_n) = 1;\ f_{j_2}(x_1, ..., x_n) = 1;\ \ldots;\ f_{j_\kappa}(x_1, ..., x_n) = 1. \right\} \quad (12)$$

Tahlil qilishda $\prod_{i=1}^{\kappa}\Delta f_{j_i}=\tilde{0}$ qiymat yagona ekanligini tekshiramiz. Agar bu yagona hisoblansa, u holda qaralayotgan qism tizim birgalikda bo‘lmaydi; 3) barcha maksimal qism tizimlarning qiymatlar tasvirlarini mantiqiy ko‘paytirishni hisoblash; 4) barcha qiymatlar tasvirini M to‘plamini shakllantirish.

Mantiqiy ifodalarni analitik o‘zgartirishga asoslangan mantiqiy tenglamalar tizimini yechishni qarab o‘tamiz. Algoritm quyidagi bosqichlarni o‘z ichiga oladi. 1) (11) tizim tenglamalaridagi ifodalarni D^1 d.n.sh. bazisdagi formulalar orqali ifodalash; 2) A_M algoritmdan foydalangan holda (12) tizimning maksimal qism tizimlarini qurish. Berilgan qism tizimning mosligini tahlil qilish, qism tizim yechimga ega ekanligini tekshirish; 3) teng kuchli tenglamalarni olib tashlash; 4) (12) ko‘rinishdagi (11) tenglamalar tizimining maksimal qism tizimlaridan d.n.sh. ko‘rinishida berilgan mantiq algebrasi funksiyalarini ko‘paytirish algoritmidan foydalangan holda (13) tenglamaga o‘tish mumkin.

$$\prod_{i=1}^{\kappa}\Delta f_{j_i}=1 \tag{13}$$

2.2-paragrafda turli bazisdagi analitik ifodalarni hosil qilish va biridan boshqasiga o‘tish masalalari yechilgan, mantiq algebrasidagi funksiyalarning bir bazisdan ikkinchi bazisga transformatsiya qilish teoremalari isbotlangan.

1-teorema. Implikatsiya operatsiyalari ketma-ketligidan iborat $\xrightarrow[i=1]{n}A_i$ mantiqiy funksiyani quyidagi ifoda shaklida yozish mumkin:

$$\xrightarrow[i=1]{n}A_i=\begin{cases}\bigwedge\limits_{i=1}^{n/2}\bar{A}_{2i-1}\vee\bigvee\limits_{j=1}^{(n/2)-1}\left(A_{2j}\bigwedge\limits_{i=j}^{(n/2)-1}\bar{A}_{2i+1}\right)\vee A_n, & \text{agar } n=2k;\\ \bigvee\limits_{j=1}^{(n/2)-1}\left(A_{2i-1}\bigwedge\limits_{i=j}^{(n/2)-1}\bar{A}_{2i}\right)\vee A_n, & \text{agar } n=2k+1,\end{cases} \tag{14}$$

2-teorema. Sheffer shtrixining $\overset{n}{\diagup}A_i$ operatsiyalari ketma-ketligidan iborat bo‘lgan mantiqiy funksiyalarni $\mathfrak{N}_1=\{x_1\wedge x_2, x_1\vee x_2, \neg x\}$ tizimidagi quyidagi d.n.sh. sifatida kabi yozish mumkin:

$$\overset{n}{\diagup}A_i=\begin{cases}\bar{A}_1\bigwedge\limits_{i=1}^{(n/2)-1}A_{2i+1}\bigvee\limits_{j=1}^{(n/2)-1}\left(\bar{A}_{2j}\bigwedge\limits_{i=j}^{(n/2)-1}A_{2i+1}\right)\vee\bar{A}_n, & \text{agar } n=2k;\\ A_1\bigwedge\limits_{i=1}^{(n-1)/2}A_{2i}\vee\bigvee\limits_{j=2}^{(n-1)/2}\left(\bar{A}_{2j-1}\bigwedge\limits_{i=j}^{(n-1)/2}A_{2i}\right)\vee\bar{A}_n, & \text{agar } n=2k+1,\end{cases} \tag{15}$$

3-teorema. Agar ekvivalentlik ifodasida “~”($\leftrightarrow$) amali ketma-ket va toq sonda bo‘lsa, u holda uni *XOR* amali bilan almashtirish mumkin, agar u juft sonda bo‘lsa umumiy formuladan oldin inkor operatsiyasini kiritish lozim. Teoremani quyidagi (16) formula shaklida ifodalash mumkin:

$$\underset{i=1}{\overset{n}{\sim}}A_i=\left\{\sum_{i=1}^{n}A_i,\ \text{agar}\ \ n=2k+1;\quad \neg\left(\sum_{i=1}^{n}A_i\right),\ \ \text{agar}\ \ n=2k\right\} \qquad (16)$$

4-teorema. Sheffer shtrixi operatsiyasidan iborat mantiqiy ifodalar ketmaketligini $\{\wedge,+,1\}$ tizimida (17) kabi yagona tarzda ifodalanadi.

$$\overset{n}{\diagup}_{i=1}A_i=\bigwedge_{i=1}^{n}A_i+\sum_{i=3}^{n}\left(\bigwedge_{j=i}^{n}A_i\right)+1 \qquad (17)$$

2.3-paragrafda (18) kabi berilgan bul tenglamalar tizimini yechish algoritmining murakkablik baholalari keltirilgan.

$$\left\{\mathfrak{A}_{11}\vee\ldots\vee\mathfrak{A}_{1t_1}=1;\cdots;\mathfrak{A}_{m1}\vee\ldots\vee\mathfrak{A}_{mt_m}=1.\right\} \qquad (18)$$

bu yerda $\mathfrak{A}_{ij}, i=\overline{1,t},\ j=\overline{1,\rho_i}$, elementar konyunksiya(e.k.).

Tenglamalar tizimini yechish uchun barcha mumkin bo‘lgan holatlarni qarab chiqishdan iborat A algoritm murakkabligi $\Psi_A\le\prod_{i=1}^{m}t_i$ bahosini qanoatlantiradi. $D_i^0=\mathfrak{A}_{i1}\vee\ldots\vee\mathfrak{A}_{it_i}$ ortogonal d.n.sh. va D_1 mukammal d.n.sh. orqali ifodalansa tenglamalar tizimini yechish murakkabligi $\Psi_{A_1}\le 2^n\sum_{i=2}^{m}t_i'$ bahosini qanoatlantiradi. Agar (18) tenglamalar tizimi qisqartirilgan d.n.sh. ifodasidan iborat bo‘lsa, tenglamalar tizimini yechish murakkabligi quyidagi (19) ko‘rinishida aniqlanadi(bu yerda $\delta'(n)\to 0$ da $n\to 0$).

$$\Psi\le(m-1)\frac{2^{2n-2}}{\left(\log_2^2 n\right)\left(\log_2\log_2 n\right)^2}\left(1+\delta'(n)\right) \qquad (19)$$

Agar (18) tenglamalar tizimi kamayadigan d.n.sh. ifodasidan iborat bo‘lsa, tenglamalar tizimini yechish murakkabligi (20) ko‘rinishda aniqlanadi ($L_i\sim 2^n n^{\log_2\log_2 n}$, $\left|S_1\left(\mathfrak{A},D_j\right)\right|\sim n^{\log_2\log_2 n}$, $\left|N_{\mathfrak{A}}\right|\sim\log_2 n$ bu yerda $\delta(n)\to 0,\ n\to 0$).

$$\Psi\le(m-1)n^{2\log_2\log_2 n}2^{2n}\left(1+\delta(n)\right) \qquad (20)$$

2.4-paragrafda Jegalkin ko‘phadini optimallashtirishda guruhlashni qo‘llaganda algebraik chiziqsizlikni kamaytirish mumkin. Bunda (21) tengliklardan foydalangan holda funksiyani (22) shaklida yoziladi. Bu yerda $\deg(F)>\deg(G_i)\ (i=\overline{1,k})$.

$$A+A=0;A\wedge 1=A;A\wedge A=A;A\wedge 0=0;A\wedge B=B\wedge A. \qquad (21)$$

$$F(x_0,x_1,\ldots,x_n)=G_1(x_0,x_1,\ldots,x_n)\wedge\cdots\wedge G_k(x_0,x_1,\ldots,x_n)=\prod_{i=0}^{k}G_i(x_0,x_1,\ldots,x_n) \qquad (22)$$

Jegalkin ko‘phadida berilgan bul funksiyaga inkor amalini kiritib elementar konyunksiyalar sonini kamaytirish mumkin lekin funksiyaning algebraik chiziqsizligi oshadi. $F(x)+1=\left(F(x)\right)'$,

$F(x)G(x)+F(x)=F(x)\big(G(x)+1\big)=F(x)\big(G(x)\big)'$ teng kuchlilik formulalar orqali inkor amalini Jegalkin ko‘phadiga kiritish mumkin. Hosil bo‘lgan ko‘phad umumlashgan Jegalkin ko‘phadi deb nomlandi.

“Shifrlash jarayonlarida akslantirishlarni baholash va ularning dasturiy ta’minoti” nomli III bobda shifrlash standartlaridagi akslantirishlarni baholash dasturiy ta’minoti hamda d.n.sh. va Jegalkin ko‘phadida berilgan bul tenglamalar tizimini yechish dasturi, blok sxemasi va murakkablik bahosi keltirilgan. Ushbu bobda zamonaviy shifrlash algoritmlari GOST R34.12-2015(Kuznechik) standart shifrlash alogoritmining mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishning optimallashtirilgan bul formulalari qarab o‘tilgan. Shuningdek bobda yuqori boblarda keltirib o‘tilgan optimallashtirilgan modellar asosida AES va GOST R34.12-2015(Kuznechik) standart simmetrik shifrlash algoritmlariga algebraik kriptotahlil o‘tkazilgan.

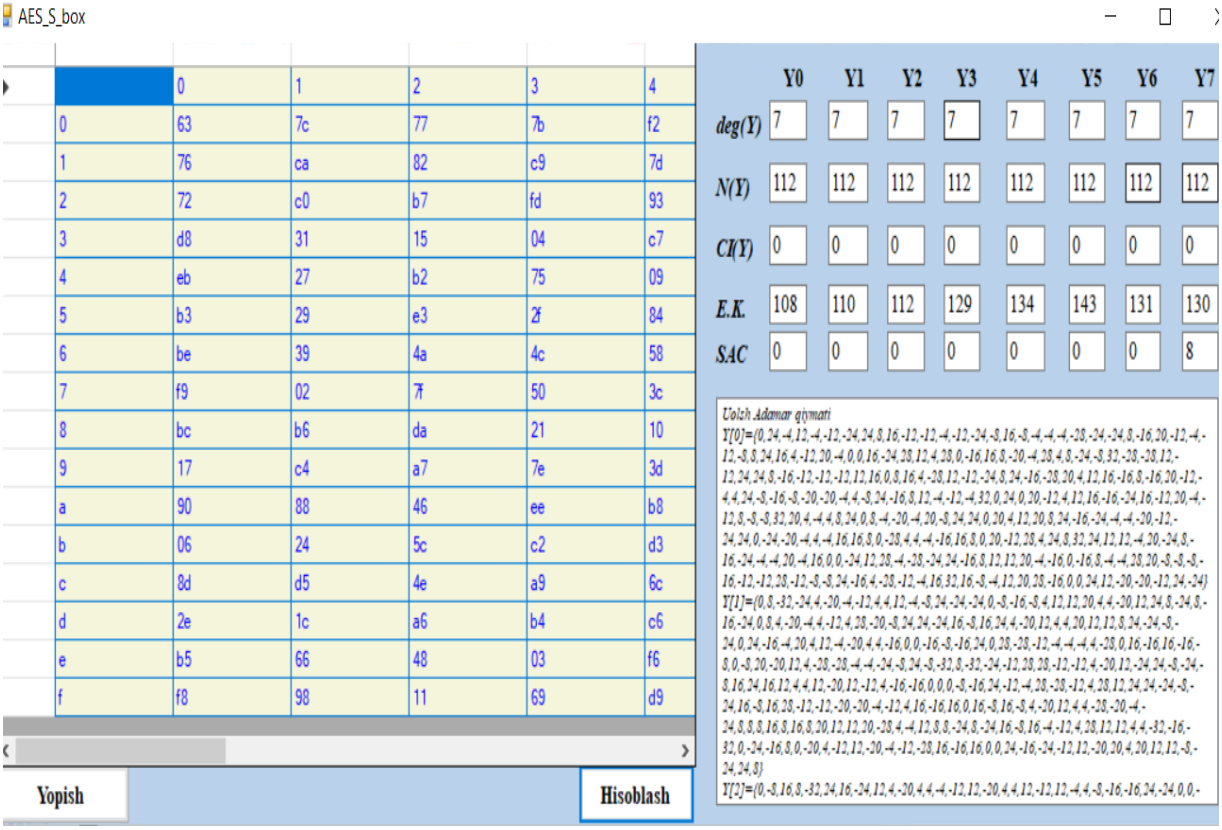
3.1-paragrafda Kuznechik shifrlash algoritmining graf-sxema algoritmi, matritsa algoritmi aniqlangan va ular asosida algoritmlardagi mikrobuyruqlarining minimal bul funksiya shakllari topilgan. Kuznechik simmetrik shifrlash algoritmidagi *X*, *S*, *L* akslantirishlari alohida qaralgan. *X* akslantirish algoritmi mikrobuyruqlarining matritsa sxemasining analitik shakli $\{Y_0=Y_1;\ Y_1=Y_2;\ Y_2=x_1Y_2\vee\overline{x}_1Y_K\}$ ko‘rinishida va bul funksiya shakli $\{Y_0=1;\ Y_1=1;\ Y_2=1;\ Y_K=\overline{x}_1;\}$ kabi aniqlangan. *S* akslantirish algoritmi mikrobuyruqlarining matritsa sxemasini analitik shakli $Y_0=Y_1;\ Y_1=Y_2;Y_2=x_1Y_2\vee\overline{x}_1Y_3;\ Y_3=Y_\kappa;$ ko‘rinishida va bul funksiya shakli $\{Y_0=1;Y_1=1;Y_2=1;Y_3=\overline{x}_1;Y_\kappa=\overline{x}_1;\}$ kabi aniqlangan. *L* akslantirish algoritmining mikrobuyruqlarining matritsa sxemasini analitik shakli $\{Y_0=Y_1;Y_1=Y_2;Y_2=\overline{x}_1x_2Y_3\vee\overline{x_1x_2}Y_4;Y_3=\overline{x}_3Y_1\vee Y_4;Y_4=Y_5\}$ ko‘rinishida va bul funksiya shakli $\{Y_0=1;Y_1=1;Y_2=1;Y_3=\overline{x}_1;Y_4=\overline{x}_1;Y_5=\overline{x}_1;Y_6=\overline{x}_1\overline{x}_2\overline{x}_3;$ $Y_7=\overline{x}_1\overline{x}_2\overline{x}_3;Y_8=\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4;\ Y_K=\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4;\}$ kabi aniqlangan.

3.2-paragrafda AES shifrlash algoritmidagi *MixColumns*, *SubBytes* akslantirishlarning matematik modelini tuzishda yordamchi bo‘lgan dasturiy maxsulotlar tafsifi keltirib o‘tilgan.

Dastur *SubBytes*, *SubBytes teskari* akslantirishlaridan xosil buluvchi 8 bul funksiyalarining d.n.sh., Jegalkin ko‘phadi shaklini va umumiy kriptografik talablar parametrlarini aniqlaydi. Shuningdek paragrafda Kuznechik shifrlash algoritmidagi *S, L* akslantirishlarning matematik modellarini tuzishda yordamchi bo‘lgan dasturiy maxsulotlar tafsifi keltirilgan(1-rasm).

3.3-paragrafda va Jegalkin ko‘phadi va d.n.sh. formulasidagi bul tenglamalar tizimini to‘liq tanlash usuli yordamida yechish algoritmining nazariy murakkabligi $T=4t+2^n\big(4nt+5t\big)$ eksponensial murakkablikka tengligi aniqlangan. Dastur tenglamalar tizimidagi algebraik chiziqsizlikni va ishlash

vaqtini ko‘rsatadi. Shuningdek paragrafda d.n.sh. ifodasidagi bul tenglamalar tizimini Karta-Karno va Kvayn minimallashtirish algoritmlarining nazariy murakkabligi $T = 5n^2/4 + 4nt + 3t$ polinomial murakkablikka tengligi hisoblangan.



1-rasm. SubBytes chiziqsiz akslantirishining dasturiy ta’minoti

3.4-paragrafda AES va Kuznechik kriptografik algoritmlarining kriptobardoshligi algebraik kriptotahlil usuli asosida baholangan.

AES algoritmi d.n.sh. formulasidagi modelda raundlar soni 3 va undan yuqori bo‘lganda, umumlashgan Jegalkin ko‘phadidagi modelda raundlar soni 6 va undan yuqori bo‘lganda, umumlashgan va guruhlashgan Jegalkin ko‘phadidagi modelda raundlar soni 5 va undan yuqori bo‘lganda shifrlash algoritmi algebraik kriptotahlil usuliga amaliy bardoshli ekanligi isbotlandi.

Kuznechik algoritmi d.n.sh. ifodasidagi modelda L akslantirishning o‘zida 2^{46} ta yangi o‘zgaruvchi va tenglama hosil bo‘lishidan ushbu modeldan algebraik kriptotahlilda qo‘llash samarali emasligi aniqlandi. Kuznechik algoritmi umumlashgan Jegalkin ko‘phadidagi modelda raundlar soni 6 va undan yuqori bo‘lganda, umumlashgan va guruhlashgan Jegalkin ko‘phadidagi modelda raundlar soni 5 va undan yuqori bo‘lganda shifrlash algoritmi algebraik kriptotahlil usuliga amaliy bardoshli ekanligi isbotlandi. Umumlashgan Jegalkin ko‘phadidagi modelda har bir akslantirishdan so‘ng qo‘shimcha tenglama va noma’lumlar hosil bo‘lishi 4-jadvalda keltirilgan. Kuznechik algoritmida raundlar soniga mos tenglamalar tizimining parametrlari 5-jadvalda keltirilgan.

Kuznechik algoritmida akslantirishlarni ifodalovchi umumlashgan Jegalkin ko‘phadidagi model parametrlari 4-jadval

Akslantirishlar	Tenglamalar soni (TS)	Noma’lumlar soni (NS)
X	256	256
S	5376	5376
L	128	128

Kuznechik algoritmini ifodalovchi umumlashgan Jegalkin ko‘phadidagi tenglamalar tizimining parametrlari 5-jadval

Raundlar	Tenglamalar soni (TS)	Noma’lumlar soni (NS)		TT ni yechish murakkabligi	TT ni saqlash uchun zarur xotira (bayt)
			2 ning darajasi shaklida		
2	11520	11520	$2^{13,4918}$	$2^{40,4755}$	
6	34560	34560	$2^{15,0768}$	$2^{45,2304}$	2^{74}
10	60288	52096	$2^{15,6688}$	$2^{47,0066}$	

XULOSA

1. Zamonaviy simmetrik shifrlash algoritmlari uchun algebraik kriptotahlil asosida shifrlash algoritmlarini umumiy kriptografik talablarga baholash qoidalari keltirilgan.

2. GOST R34.12-2015, AES, A5/1 simmetrik shifrlash algoritmlari uchun algebraik kriptotahlil usuli asosida optimallashtirilgan matematik modellar ishlab chiqilgan va umumiy kriptografik talablarga baholash keltirilgan.

3. GOST R34.12-2015 shifrlash algoritmidagi *L* akslantirishi AES shifrlash algoritmidagi *MixColums* akslantirishidan samaraliroq ekanligi 1-4-tasdiqlar natijasi sifatida isbotlangan, xususan:

- Chiquvchi har bir bitning, kiruvchi bit qiymatlarga bog‘liqligi minimal ***5.71*** barobar yuqori.
- Kiruvchi har bir bitning, chiquvchi nechta bit qiymatlarga bog‘liqligi ***5.1*** barobar yuqori ekanligi aniqlangan.

4. Mantiqiy tenglamalar tizimlarining maksimal qism tizimini topish masalasi hal qilindi, buning uchun monoton mantiqiy funksiyaning maksimal yuqori nolini topish algoritmi taklif qilindi hamda *n* o‘lchovli kub to‘plamlarida *f* monoton funksiyalarining qiymatlarini hisoblashning samarali tartibi ishlab chiqilgan.

5. Mantiqiy algebrada monoton funksiyalarning maksimal yuqori nolini izlash asosida mantiqiy tenglamalar tizimining yuqori qism tizimlarini yechish algoritmi ishlab chiqildi.

6. Turli bazisdagi analitik ifodalarni hosil qilish va transformatsiya masalalari yechilgan, mantiq algebrasidagi funksiyalarning turli bazislarda ifodalash va o‘zgartirishga oid teoremalar isbotlangan.

7. Jegalkin ko‘phadi shaklidagi bul funksiyalarni optimallashtirish usullari va algoritmlari ishlab chiqilgan. Jegalkin ko‘phadi shaklidagi bul tenglamasini yechish bosqichlari keltirilgan.

8. Kuznechik shifrlash algoritmi mikrobuyruqlari ketma-ketligini mikrokontrollerlarga o‘tkazishda optimallashtirilgan bul formulalari yaratilgan.

9. Kuznechik va AES-128 standartidagi akslantirishlarni umumiy kriptografik parametrlarini hisoblovchi dasturiy ta’minot yaratilgan.

10. Jegalkin ko‘phadi va minimallashtirilgan d.n.sh. ko‘rinishidagi bul tenglamalar tizimini yechish dasturiy ta’minoti ishlab chiqilgan. To‘liq tanlash usuli yordamida bul tenglamalar tizimini yechish murakkabligi hisoblab chiqilgan.

11. Kuznechik va AES shifrlash algoritmlari uchun turli bazisda aniqlangan matematik modellar yordamida algebraik kriptotahlil o‘tkazildi. O‘tkazilgan tahlillarga muvofiq raundlar soni 6 va undan yuqori bo‘lgan Kuznechik va AES shifrlash algoritmlari algebraik kriptotahlil usuliga amaliy bardoshli ekanligi isbotlangan.

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

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

БЕРДИМУРОДОВ МАНСУР АЛИШЕРОВИЧ

ЛОГИЧЕСКИЕ МЕТОДЫ РЕШЕНИЯ ЗАДАЧ КРИПТОАНАЛИЗА

05.01.05–Методы и системы защиты информации. Информационная безопасность (физико-математические науки)

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

Ташкент-2023

Тема диссертации доктора философии (PhD) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за №B2020.4.PhD/FM553.

Диссертация выполнена в Национальном Университете Узбекистана имени Мирзо Улугбека.

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

Научный руководитель:	**Кабулов Анвар Василович** доктор техническим наук, профессор
Официальные оппоненты:	**Абдурахимов Бахтиёр Файзиевич** доктор физико-математических наук, профессор
	Абдусобир Саидов А. доктор технических наук, профессор
Ведущая организация:	**“UNICON.UZ” Государственное унитарное предприятие**

Защита диссертации состоится «____» _____2023 года в ____ часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24, факс: (+99871) 246-53-21, e-mail: nauka@nuu.uz).

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

Автореферат диссертации разослан «____» _____2023 года.
(протокол рассылки №_____ от «____» _____2023 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.

Г.У. Жураев
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.ф.-м.н.

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В мире как результат проводимых в глобальном масштабе многочисленных научных и практических исследований проблемы криптографии и криптоанализа в большинстве случаев сводятся к вопросам изучения свойств алгоритмов шифрования, их алгебраического выражения. Оценка толерантности алгоритма шифрования и разработка криптографических отображений являются объектом исследований в таких областях, как прикладная математика, дискретная математика, математическое моделирование и объектно-ориентированное программирование. Развитие методов криптоанализа и вычислительной техники служит основой для легкого решения задач криптоанализа и снижения устойчивости алгоритмов шифрования. В связи с этим принимаемый во внимание рост угроз информационным системам, оценка надежности алгоритмов шифрования, используемых на практике, остается одной из важных задач.

В настоящее время определение особенностей отображения алгоритмов криптографического шифрования, оценка криптостойкости алгоритмов шифрования методами криптоанализа является одной из актуальных проблем криптоанализа. В этом аспекте все большее значение приобретают алгебраическое выражение криптографических отображений, изучение их числовых характеристик. В связи с этим основу целенаправленных научных исследований должны составлять оценка толерантности алгоритмов шифрования, принятых в качестве национального стандарта, с использованием современных методов криптоанализа и создание новых национальных алгоритмов шифрования.

В Республике Узбекистан наибольшее внимание уделяется современным направлениям криптологии, требующим научного и практического применения фундаментальных наук. В частности, особая значимость придается созданию защищенных систем передачи и обработки информации, базирующейся на достижениях в области криптографии и системы разработки алгоритмов. Наряду с этим выполняются работы, направленные на определение основных задач по проведению на уровне международных стандартов научных исследований по приоритетным направлениям «Прикладная математика и математическое моделирование». Проведение научных исследований на уровне международных стандартов по приоритетным направлениям «Функциональный анализ, алгебра, дифференциальные уравнения, математическая физика, математическое моделирование, вычислительная математика и дискретная математика, теория вероятностей и математическая статистика» является одной из основных задач Института математики им. В.И.Романовского при Академии наук Республики Узбекистан[2]. Для обеспечения ее реализации

[2] Постановление Президента Республики Узбекистан №ПП-4708 от 7 мая 2020 г. «О мерах по повышению качества образования и развитию научных исследований в области математики».

важное значение имеет создание оптимизированных математических моделей современных алгоритмов симметричного шифрования на основе методов алгебраического криптоанализа и на их базе – разработка и применение логических методов для оценки общих криптографических требований, а также создание их программного обеспечения.

Настоящее диссертационное исследование в определенной степени служит выполнению задач, определенных в Указах Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-60 от 28 января 2022 г. «О Стратегии развития Нового Узбекистана на 2022–2026 годы», Постановлениях Президента Республики Узбекистан №ПП-2789 от 17 февраля 2017 г. «О мерах по дальнейшему совершенствованию деятельности Академии наук, организации, управления и финансирования научно-исследовательской деятельности», №ПП-2909 от 20 апреля 2017 г. «О мерах по дальнейшему развитию системы высшего образования», №ПП-3682 от 27 апреля 2018 г. «О мерах по дальнейшему совершенствованию системы практического внедрения инновационных идей, технологий и проектов», а также в других нормативно-правовых документах, принятых в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствии с приоритетным направлением развития науки и технологий Республики Узбекистан IV. «Развитие информатизации и информационно-коммуникационных технологий».

Степень изученности проблемы. Вопросы оценки методами криптоанализа рассматривались в научных работах таких зарубежных и отечественных ученых, как: А.Бирюков, Д.Ховратович, N.T.Courtois, Н.Фергюсон, Р.Шреппель, D.Whiting, С.А.Кабаков, О.Е.Александров. Л.Бабенко, М.Арипов, Б.Абдурахимов, Г.Туйчиев, А.Саттаров, Д.Курьязов и др.

В работах Туйчиева Г., Курьязова Д., Саттарова А., Алексея Бирюкова, Дмитрия Ховратовича и др. по оценке алгоритмов шифрования по общим криптографическим требованиям, а в работах Куртуа Н.Т., Алексея Бирюкова, Дмитрия Ховратовича и других по методам алгебраического криптоанализа в сравнении со стандартными алгоритмами шифрования AES, ГОСТ Р34. 12-2015 (Кузнечик), получены эффективные результаты.

Исследования, связанные с вопросами алгоритма шифрования и оценки стойких криптографических отображений, были проведены в нашей стране и зарубежом рядом ученых, в частности, такими, как A.Youssef, N.Courtois, Б.Шнайер, К.Шеннон, G.Murtaza, I.Hussain, J.Nakahara, Ж.Рижмен, K.Chand, K.Gupta, K.Nyberg, M.Malik, Hasan Omar, Zhou Yuyang, P.Junod, М.Арипов, М.Каримов, Б.Абдурахимов, Р.Олейников, Т.Чалкин, Г.У.Жўраев, Д.Курьязов, А. Саттаров, А.В.Кабулов и др.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертация выполнена в соответствии с планом научных исследований Национального университета Узбекистана в рамках научно-исследовательских проектов №Ф3-201906117. «Программное обеспечение для мониторинга выявления влияния экологических ситуаций на сельскохозяйственное производство Аральского моря» и БВ-М-Ф4-004. «Разработка принципов алгоритмизации управления сложными системами на основе алгебры функциональных таблиц».

Целью исследования являются анализ отображений и их толерантности в криптографических алгоритмах шифрования AES и ГОСТ Р34.12-2015 (Кузнечик), оценка с использованием алгебраического метода криптоанализа, а также создание и оценка сложности математической модели на различных основаниях с использованием логических методов.

Задачи исследования:

создать оптимизировонные математические модели современных алгоритмов симметричного шифрования на основе методов алгебраического криптоанализа;

разработать логические методы для оценки общих криптографических требований на основе созданных математических моделей современных алгоритмов симметричного шифрования;

разработать алгоритмы создания и решения систем булевых уравнений, заданных в различных базисах математических моделей современных алгоритмов симметричного шифрования, а также оценить их сложность;

разработать критерии и алгоритмы преобразования отображений в алгоритмах симметричного блочного шифрования AES и ГОСТ Р34.12-2015 (Кузнечик) в булевы функции на разных базах;

разработать программное обеспечение для решения системы булевых уравнений, заданных полиномами Жегалкина и дизъюнктивными нормальными формами отображений в стандарте AES-128 и ГОСТ Р34.12-2015 (Кузнечик);

выразить алгоритм шифрования Кузнечика в оптимизированных формулах булевой алгебры при передаче последовательности микрокоманд на микроконтроллеры;

разработать алгоритм решения систем логических уравнений и определить максимальную совместную подсистему систем логических уравнений на основе поиска максимального верхнего нуля логических булевых монотонных функций;

осуществить алгебраический криптоанализ на основе разработанных оптимизированных математических моделей.

Объектом исследования являются криптографические алгоритмы, математические модели отображения, системы булевых уравнений, булевы функции, формы микрокоманд алгоритмов.

Предметом исследования являются математические модели отображения, криптостойкость криптоалгоритмов, алгебраические и логические процессы, анализ и исследование криптоанализа, булевы таблицы криптосистем и булевы функции криптоалгоритмов, микрокоманды криптоалгоритмов.

Методы исследования. В исследовании применяются криптоанализ, теория булевых уравнений, теория микрокоманд, логические модели, методы алгебраической и математической логики, методы объектно-ориентированного программирования.

Научная новизна диссертационного исследования заключается в следующем:

созданы оптимизированные математические модели на основе методов алгебраического криптоанализа алгоритмов AES, ГОСТ Р34.12-2015 (Кузнечик), A5/1;

вычислена оценка общих криптографических требований современных алгоритмов симметричного шифрования AES, ГОСТ Р34.12-2015 (Кузнечик) на основе их математических моделей и проведен алгебраический криптоанализ на основе различных логических базисов алгоритмов

созданы оптимизированные формулы булевых функций при передаче последовательности микрокоманд на микроконтроллеры алгоритма шифрования Кузнечик;

разработаны критерии и алгоритмы приведения отображений в алгоритмах симметричного шифрования AES, ГОСТ Р34.12-2015 (Кузнечик) и A5/1 к булевым функциям, заданных в различных базисах, а также доказана теорема трансформации логических формул с одного базиса на другой;

разработаны алгоритмы решения систем булевых уравнений на основе поиска максимального верхнего нуля монотонных булевых функций и оценена их сложность;

Практические результаты исследования заключаются в следующем:

построены булевых таблицы на основе граф-схем алгоритмов в криптосистемах;

созданы оптимизированные формулы булевых функций при передаче последовательности микрокоманд алгоритмов шифрования Кузнечик на микроконтроллеры;

расработаны оптимизированные математические модели отображений в стандартах AES-128 и ГОСТ Р34.12-2015 (Кузнечик);

проведен алгебраический криптоанализ и дана оценка криптостойкости на основе математических моделей по стандартам AES-128 и ГОСТ Р34.12-2015 (Кузнечика);

построена математическая модель отображений в алгоритмах шифрования на основе функций алгебры логики;

разработано программное обеспечение для решения систем нелинейных булевых уравнений, заданных полиномами Жегалкина и д.н.ф.

Достоверность результатов исследования обоснована строгостью математических рассуждений, использованием дискретной математики и методов математической логики, созданием математических моделей современных алгоритмов симметричного шифрования, разработкой логических методов для оценки общих криптографических требований.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования заключается в том, что на основе созданных оптимизированных математических моделей современных алгоритмов симметричного шифрования разработаны логические методы оценки общих криптографических требований, на основе моделей которых осуществляется алгебраический криптоанализ.

Практическая значимость результатов исследования заключается в том, что во встроенных микропроцессорных системах создаются оптимизированные логические формулы при передаче последовательности микрокоманд алгоритма шифрования Кузнечика на микроконтроллеры и это основано на простоте их применения в аппаратно-программных средствах.

Внедрение результатов исследования. На основе оптимизированных математических моделей, созданных для современных алгоритмов шифрования AES, Кузнечик, A5/1, и результатов, полученных при оценке общих криптографических требований:

Оптимизированная математическая модель алгоритмов шифрования AES, Кузнечик и результаты оценки общих криптографических требований используются в проекте OT-Atex-2018-486 «Реализация систем логического управления и защиты информации на основе программированных логических контроллеров и автоматизированной логической системы CAD их проектирования» при анализе и оптимизации форм (Справка 04/10-2807 от 17 май 2022 г. Национального университета Узбекистана им. Мирзо Улугбека). Применение научных результатов позволило оптимально реализовать и проанализировать алгоритмы шифрования на базе микроконтроллера.

правила оценки алгоритмов шифрования для современных симметричных алгоритмов шифрования на соответствие общим криптографическим требованиям, использованы в процессе оценки криптографических алгоритмов с применением современных методов криптоанализа в рамках проекта «Создание криптографических алгоритмов» проводимого в «UNICON.UZ» ГУП. Также данные, полученные из решений применения критериев и алгоритмов приведения к булевым функциям в разных базисах отображений в алгоритме симметричного блочного шифрования ГОСТ Р34.12-2015 использованы в «UNICON.UZ» ГУП при оценке устойчивости алгоритмов симметричного блочного шифрования, применяемых в национальных защищенных

системах (Справка 5-3/945 от 10 июнь 2022 г. «UNICON.UZ» ГУП). Применение научных результатов позволило оценить и проанализировать устойчивость алгоритмов симметричного блочного шифрования, используемых в системах национальной безопасности.

Апробация результатов исследования. Результаты данного исследования обсуждались на 10 научно-практических конференциях, в том числе 6 международных и 4 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По основным результатам исследования опубликовано всего 18 научных статей, в том числе 8 – статей в научных изданиях, из них из них 5 – в республиканских и 4 (в базе данных scopus) – в зарубежных журналах, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов диссертации доктора философии (PhD). Получены также 4 свидетельства о регистрации программных средств, созданных для ЭВМ.

Структура и объем диссертации. Диссертационная работа состоит из введения, трех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 114 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснованы актуальность и востребованность темы диссертации, сформулированы цель и задачи исследования, охарактеризованы объект и предмет исследования, раскрыто соответствие исследования приоритетным направлениям развития науки и технологий республики, определены научная новизна и практические результаты исследования, обоснована достоверность полученнных результатов, показаны научная и практическая значимость полученных результатов, внедрение их в практику, даны сведения по опубликованным работам и структуре диссертации.

В первой главе диссертации под названием **«Создание оптимизированных математических моделей современных алгоритмов симметричного шифрования для алгебраического криптоанализа и оценка к общим криптографическим требованиям»** рассмотрены *SubBytes, ShiftRows, MixColumns* и *AddRoundKey* отображения алгоритма шифрования AES, алгоритм построения математической модели отображений *S, L, X* в стандартном алгоритме ГОСТ Р34.12-2015(Кузнечик) на основе булевых функций и математическая модель каждого отображения в полиноме Жегалкина и дизъюнктивной нормальной форме (д.н.ф.). На основе булевых функций проанализирована оценка отображений в соответствии с общими криптографическими требованиями. В параграфе 1.1 дана оценка алгоритмов шифрования на основе алгебраического криптоанализа с общими криптографическими требованиями.

Представлены некоторые математические понятия, необходимые для оценки булевых функций и отображений. В параграфе 1.2 описаны создание оптимизированных математических моделей криптографического алгоритма AES и оценка общих криптографических требований, а также построены математические модели на основе булевых функций каждого отображения в алгоритме шифрования.

Показано, что отображение *AddRoundKey* – это отображение добавления ключа раунда. Входящие и исходящие биты отображения определяются следующим образом: $y_j = x_j \oplus k_{i\,j}$ (здесь $K_i = (k_{i0}, k_{i1}, \cdots, k_{i127}), (i = \overline{0,10}),\ (j = \overline{0,127})$ ключи раунда). Входящие a_i и исходящие b_i биты нелинейного отображения *SubBytes* могут принимать 256 различных значений. В порядке возрастания входящих a_i байтовых значений в соответствии с исходящими b_i байтовыми значениями формируется таблица истинности 8 булевых функций с 8 переменными. Здесь $i = 8 \cdot t,\ t = \overline{0,15}$. *SubBytes* исходящий в нелинейном отображении $b_i (i = \overline{0,15})$ байт определяется как

$$\left.\begin{array}{l} y_{i*8} = S_0(a_i), y_{i*8+1} = S_1(a_i), \cdots, y_{i*8+7} = S_7(a_i) \\ b_i = y_{i*8} \,||\, y_{i*8+1} \,||\, y_{i*8+2} \,||\, y_{i*8+3} \,||\, y_{i*8+4} \,||\, y_{i*8+5} \,||\, y_{i*8+6} \,||\, y_{i8+7} \end{array}\right\} \quad (1)$$

На основании значения определенных выходных $S_i(x)$ функций совершенная дизъюнктивная нормальная форма была приведена к минимальной д.н.ф. элементарных конъюнкций(э.к.) с использованием методов минимизации Карты-Карно и Квайна. Из нелинейных *отображений SubBytes* и *Subbytes* в алгоритме шифрования AES построены оптимизированные математические модели выходных y_i $(i = \overline{0,7})$ битов, заданных минимальной д.н.ф. и алгебраической нормальной формой(а.н.ф.). Функции алгебры логики, представляющие нелинейные отображения *SubBytes* и *обратный Subbytes*, были оценены в соответствии с общими криптографическими требованиями. Оценки общих криптографических требований булевой функции, дающей нелинейное представление *SubBytes*, приведены в табл. 1.

SubBytes отображение $(i = 8 \cdot t,\ t = \overline{0,15})$ Таблица 1

SubBytes	y_i	y_{i+1}	y_{i+2}	y_{i+3}	y_{i+4}	y_{i+5}	y_{i+6}	y_{i+7}
Сбалансированность	+	+	+	+	+	+	+	+
Регулярность	+							
Алгебраическая нелинейность в а.н.ф.	7	7	7	7	7	7	7	7
Нелинейность $N(y)$	112	112	112	112	112	112	112	112

Алгебраический иммунитет	2							
Корреляционный иммунитет	0	0	0	0	0	0	0	0
Количество э.к в а.н.ф.	108	110	112	129	134	143	131	130
Алгебраическая нелинейность в д.н.ф.	7	8	7	7	8	7	7	7
Количество э.к в д.н.ф.	55	52	59	49	54	50	53	49

ShiftRows(SR) – это отображение байтового сдвига и выражение отображения в виде битов определяется следующим образом:

$$\left.\begin{aligned} &y_k = x_k; y_{8+k} = x_{40+k}; y_{16+k} = x_{80+k}; y_{24+k} = x_{120+k}; y_{32+k} = x_{32+k}; y_{40+k} = x_{72+k};\\ &y_{48+k} = x_{112+k}; y_{56+k} = x_{24+k}; y_{64+k} = x_{64+k}; y_{72+k} = x_{104+k}; y_{80+k} = x_{16+k}; y_{88+k} = x_{56+k};\\ &y_{96+k} = x_{96+k}; y_{104+k} = x_{8+k}; y_{112+k} = x_{48+k}; y_{120} = x_{88+k};\text{ здесь } k = \overline{0,7} \end{aligned}\right\} (2)$$

Для перевода байтов $b_j\,(j = \overline{0,15})$, исходящих с отображения ***MixColums***(MC), можно использовать следующие уравнения:

$$\left.\begin{aligned} &f(x) = (t_7t_6t_5t_4t_3t_2t_1t_0); \quad 0\bullet f(x) = 0; \quad 01\bullet f(x) = f(x);\\ &02\bullet f(x) = x\bullet f(x) = \begin{cases} (t_6t_5t_4t_3t_2t_1t_0 0) \text{ если } t_7 = 0 \\ (t_6t_5t_4t_3t_2t_1t_0 0)\oplus(00011011) \text{ если } t_7 = 1 \end{cases}\\ &03\bullet f(x) = \{01\oplus 10\}\bullet f(x) = \{01_2\bullet f(x)\}\oplus\{10_2\bullet f(x)\} = f(x)\oplus x\bullet f(x) \end{aligned}\right\} (3)$$

Утверждения уравнений (1)–(2) доказаны с помощью математических моделей формул функции алгебры логики выходящих битов $y_j\,(j = \overline{0,127})$ из отображения.

1-е утверждение. Каждый бит, исходящий из линейного отображения *MixColumns*, – значение зависимости от количества входящих битовых значений, соответственно равное значениям {5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5, 5, 5, 5, 7, 7, 5, 7, 5}.

2-е утверждение. Каждый бит, входящий в линейное отображение *MixColumns*, – значение зависимости от количества исходящих битовых значений, соответственно равное значениям {11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5, 11, 5, 5, 5, 5, 5, 5, 5}.

В параграфе 1.3 изложено построение оптимизированных математических моделей стандартного криптографического алгоритма ГОСТ Р34.12-2015 и дана оценка общих криптографических требований.

Алгоритм сложения ключей ($X(K,M)$) криптографического алгоритма Кузнечик определен по следующим формулам (4).

$$\left.\begin{array}{l} X(K_i, M) = K_i \oplus M;\ (i = \overline{1,10})M = (m_0 \| m_1 \| \ldots \| m_{127}); \\ K_i = (k_0 \| k_1 \| \ldots \| k_{127});\ X = (k_0 \| k_1 \| \ldots \| k_{127}) \oplus (m_0 \| m_1 \| \ldots \| m_{126} \| m_{127}) \end{array}\right\} \quad (4)$$

Построена математическая модель y_i $(i = \overline{0,127})$ битов, выходящих из нелинейного S-отображения в виде булевой функции с 8 переменными (a,b,c,d,e,f,g,h). Функции алгебры логики, представляющие нелинейные отображения S и S^{-1}, оценены по общим S-криптографическим требованиям. Оценка отображения криптографических требований приведена в табл. 2.

S нелинейное отображение $(i = 8 \cdot t,\ t = \overline{0,15})$ Таблица 2

S	y_i	y_{i+1}	y_{i+2}	y_{i+3}	y_{i+4}	y_{i+5}	y_{i+6}	y_{i+7}
Сбалансированность	+	+	+	+	+	+	+	+
Регулярность	+							
Алгебраическая нелинейность в а.н.ф.	7	7	7	7	7	7	7	7
Нелинейность $N(y)$	104	106	116	104	110	106	102	104
Алгебраический иммунитет	3							
Корреляционный иммунитет	0	0	0	0	0	0	0	0
Количество э.к в а.н.ф.	137	132	143	135	122	125	123	122
Алгебраическая нелинейность в д.н.ф.	7	7	7	7	7	8	7	7
Количество э.к в д.н.ф.	53	50	49	49	62	55	52	48

Доказаны 3,4 утверждения на основе общих математических моделей линейного отображения L.

3-е утверждение. Значение взаимосвязи нескольких входящих значений бита с каждым битом выходящего из L-линейного отображения равно значениям {98, 100, 87, 82, 88, 97, 97, 93, 100, 91, 103, 104, 92, 87, 99, 107, 102, 99, 91, 102, 101, 96, 103, 87, 101, 96, 106, 96, 102, 96, 90, 101, 106, 95, 88, 97, 91, 90, 100, 102, 103, 97, 101, 96, 92, 94, 90, 100, 106, 102, 103, 101, 94, 106, 100, 106, 93, 96, 96, 90, 95, 97, 93, 87, 99, 107, 102, 101, 106, 104, 106, 99, 105, 102, 102, 100, 106, 104, 101, 106, 102, 103, 87, 100, 99, 95, 99, 108, 106, 95, 91, 103, 99, 97, 95, 101, 105, 98, 93, 99, 94, 92, 101, 91, 98, 95, 98, 94, 91, 93, 97, 101, 99, 99, 88, 85, 82, 94, 87, 93, 65, 62, 40, 42, 44, 54, 57, 59}.

4-е утверждение. Значение взаимосвязи нескольких выходящих значений бита с каждым битом входящего в L-линейное отображение равно значениям {123, 101, 106, 89, 103, 97, 108, 94, 105, 107, 98, 95, 105, 68, 87, 77, 106, 102, 95, 103, 93, 90, 100, 81, 109, 80, 90, 107, 77, 86, 94, 69, 109, 99, 108, 105, 108, 104, 106, 95, 102, 103, 104, 107, 105, 83, 103, 88, 93, 97, 77, 75,

100, 91, 89, 95, 118, 109, 100, 104, 104, 100, 91, 110, 77, 74, 80, 76, 83, 88, 94, 94, 114, 111, 107, 105, 108, 86, 103, 95, 114, 103, 115, 112, 112, 90, 101, 97, 116, 77, 83, 116, 72, 74, 64, 78, 114, 93, 99, 107, 95, 101, 98, 81, 114, 118, 76, 99, 115, 62, 86, 65, 123, 79, 83, 93, 101, 86, 115, 93, 70, 56, 71, 75, 80, 60, 83, 84}.

Определена общая аналитическая форма алгоритма шифрования Кузнечик. В определенном аналитическом виде сформулированы неизвестные уравнения, приведенные в табл. 3.

Общие параметры алгоритма Кузнечик Таблица 3.

Раунд	Ключ неизвестный	Всего неизвестный	$def(y)$	Количество	
				Э.к. в а.н.ф.	Э.к. в д.н.ф.
1	128	$2\cdot128$	7	$143\cdot107$	$\le r_1 = 2^8\cdot62\cdot2^{106}+1$
2	$2\cdot128$	$3\cdot128$	49	$(143\cdot107)^2\cdot107$	$\le r_2 = r_1^8\cdot62\cdot2^{106}+1$
n	$128\cdot n$	$(n+1)\cdot128$	7^n	$(143\cdot107)^7\cdot107$	$\le r_n = r_{n-1}^{\ 8}\cdot62\cdot2^{106}+1$
10	$10\cdot128$	$11\cdot128$	1408	$(143\cdot107)^{10}\cdot107$	$\le r_{10} = r_9$
Всего	1280	1408	1408	$\approx 7.53\cdot10^{43}$	

В параграфе 1.4 описано построение математических моделей алгоритма потокового шифрования A5/1 на различных базисах. На каждом этапе вычисления ключевого бита определяется $m = maj(x_8, y_{10}, z_{10})$ мажорное значение. Предложены математические модели на основе алгоритма определения больших значений и булевой функции в $\{\vee,\wedge,\neg\}$ и $\{\oplus,\wedge,1\}$ базисах: $m = x_8y_{10} \vee x_8z_{10} \vee y_{10}z_{10}$; $m = x_8y_{10} \oplus x_8z_{10} \oplus y_{10}z_{10}$.

Сдвиг в регистре X. Независимо от того, является ли значение x_8 бита в регистре *X* равным мажорному значению или нет, $\{\oplus,\wedge,1\}$ базис процесса сдвига определяется в виде полиномиальной математической модели (5) Жегалкина по формуле

$$\left.\begin{array}{l} t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}; \\ x_i = (m \leftrightarrow x_8)x_{i-1} \vee \overline{(m \leftrightarrow x_8)}x_i = x_{i-1} \oplus x_8x_i \oplus x_8x_{i-1} \oplus mx_i \oplus mx_{i-1}; \\ (\text{здесь } i = \overline{18,1}); \qquad x_0 = t \oplus x_8x_0 \oplus x_8t \oplus mx_0 \oplus mt \end{array}\right\} \quad (5)$$

а $\{\vee,\wedge,\neg\}$ базис – в виде математической модели (6) в д.н.ф. по формуле

$$\left.\begin{array}{l} t = x_{13}x_{16}x_{17}\overline{x_{18}} \vee x_{13}\overline{x_{16}}\,\overline{x_{17}}\,\overline{x_{18}} \vee x_{13}x_{16}\overline{x_{17}}x_{18} \vee x_{13}\overline{x_{16}}x_{17}x_{18} \vee \\ \vee\overline{x_{13}}x_{16}\overline{x_{17}}\,\overline{x_{18}} \vee \overline{x_{13}}x_{16}x_{17}x_{18} \vee \overline{x_{13}}\,\overline{x_{16}}x_{17}\overline{x_{18}} \vee \overline{x_{13}}\,\overline{x_{16}}\,\overline{x_{17}}x_{18} \\ x_i = (m \leftrightarrow x_8)x_{i-1} \vee \overline{(m \leftrightarrow x_8)}x_i = x_i\,x_{i-1} \vee mx_8x_{i-1} \vee m\overline{x_8}x_i \vee \\ \vee\overline{m}x_8x_i \vee \overline{m}\,\overline{x_8}x_{i-1}; \qquad (\text{здесь } i = \overline{18,1}) \\ x_0 = (m \leftrightarrow x_8)t \vee \overline{(m \leftrightarrow x_8)}x_0 = x_0t \vee mx_8t \vee m\overline{x_8}x_0 \vee \overline{m}x_8x_0 \vee \overline{m}\,\overline{x_8}t \end{array}\right\}. \quad (6)$$

Сдвиг в регистре Y. Процесс сдвига регистра Y определяется в виде базиса $\{\oplus,\wedge,1\}$ полиномиальной математической модели (7) Жегалкина по формуле

$$\left.\begin{array}{l} t = y_{20} \oplus y_{21}; \quad (\text{здесь } i = \overline{21,1}); \\ y_i = (m \leftrightarrow y_{10}) y_{i-1} \vee \overline{(m \leftrightarrow y_{10})} y_i = y_{i-1} \oplus y_{10} y_i \oplus y_{10} y_{i-1} \oplus m y_i \oplus m y_{i-1}; \\ y_0 = (m \leftrightarrow y_{10}) t \vee \overline{(m \leftrightarrow y_{10})} y_0 = mt \oplus y_{10} t \oplus m y_0 \oplus y_{10} y_0 \oplus t; \end{array}\right\} \quad (7)$$

а $\{\vee,\wedge,\neg\}$ базис – виде оптимизированной математической модели в (8) д.н.ф. по формуле

$$\left.\begin{array}{l} t = y_{20} \oplus y_{21} = y_{20}\overline{y_{21}} \vee \overline{y_{20}} y_{21}; \; y_i = (m \leftrightarrow y_{10}) y_{i-1} \vee \overline{(m \leftrightarrow y_{10})} y_i = y_i\, y_{i-1} \vee \\ \vee m y_{10} y_{i-1} \vee m\overline{y_{10}} y_i \vee \overline{m} y_{10} y_i \vee \overline{m}\,\overline{y_{10}} y_{i-1}; \quad (\text{здесь } i = \overline{21,1}); \\ y_0 = (m \leftrightarrow y_{10}) t \vee \overline{(m \leftrightarrow y_{10})} y_0 = y_0 t \vee m y_{10} t \vee m\overline{y_{10}} y_0 \vee \overline{m} y_{10} y_0 \vee \overline{m}\,\overline{y_{10}} t \end{array}\right\} \quad (8)$$

Сдвиг в регистре Z. Процесс сдвига регистра Z определяется в виде базиса $\{\oplus,\wedge,1\}$ полиномиальной математической модели (9) Жегалкина по формуле

$$\left.\begin{array}{l} t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}; \; z_i = (m \leftrightarrow z_{10}) z_{i-1} \vee \overline{(m \leftrightarrow z_{10})} z_i = \\ = z_{i-1} \oplus z_{10} z_i \oplus z_{10} z_{i-1} \oplus m z_i \oplus m z_{i-1}; \quad \left(\text{здесь } i = \overline{22,1}\right) \\ z_0 = (m \leftrightarrow z_{10}) t \vee \overline{(m \leftrightarrow z_{10})} z_0 = mt \oplus z_{10} t \oplus m z_0 \oplus z_{10} z_0 \oplus t; \end{array}\right\} \quad (9)$$

а $\{\vee,\wedge,\neg\}$ базис – в виде оптимизированной математической модели в (10) д.н.ф. по формуле

$$\left.\begin{array}{l} t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22} = z_7 z_{20} z_{21} \overline{z_{22}} \vee z_7 \overline{z_{20}}\,\overline{z_{21}}\,\overline{z_{22}} \vee z_7 z_{20} \overline{z_{21}} z_{22} \vee z_7 \overline{z_{20}} z_{21} z_{22} \vee \\ \vee \overline{z_7} z_{20} \overline{z_{21}}\,\overline{z_{22}} \vee \overline{z_7} z_{20} z_{21} z_{22} \vee \overline{z_7}\,\overline{z_{20}} z_{21} \overline{z_{22}} \vee \overline{z_7}\,\overline{z_{20}}\,\overline{z_{21}} z_{22}; \; z_i = (m \leftrightarrow z_{10}) z_{i-1} \vee \\ \vee \overline{(m \leftrightarrow z_{10})} z_i = z_i\, z_{i-1} \vee m z_{10} z_{i-1} \vee m\overline{z_{10}} z_i \vee \overline{m} z_{10} z_i \vee \overline{m}\,\overline{z_{10}} z_{i-1}; (\text{здесь } i = \overline{22,1}) \\ z_0 = (m \leftrightarrow z_{10}) t \vee \overline{(m \leftrightarrow z_{10})} z_0 = z_0 t \vee m z_{10} t \vee m\overline{z_{10}} z_0 \vee \overline{m} z_{10} z_0 \vee \overline{m}\,\overline{z_{10}} t; \end{array}\right\} \quad (10)$$

Во второй главе диссертации предложен алгоритм решения системы булевых уравнений на основе нахождении максимального верхнего нуля монотонных функций в логической алгебре. Рассмотрены аналитические преобразования в минимизации логических функций класса дизъюнктивных нормальных форм, некоторые аналитические формулы преобразования логических выражений в общую форму. Решены задачи формирования и трансформации различных аналитических выражений и доказаны теоремы преобразования функций логической алгебры из одного базиса в другой. Описаны методы оптимизации полинома Жегалкина.

В параграфе 2.1. на основе задачи нахождения максимального верхнего нуля монотонных булевых функций решена задача нахождения максимальных совместных подсистем булевой системы уравнений. Разработана A_M модификация алгоритма A_K Катериночкиной для задачи

поиска м.в.н монотонных логических функций.

Решение задачи нахождения максимальных совместных подсистем логической булевой системы уравнений

$$M = \left\{ f_1(x_1, x_2, ..., x_n) = 1;\ f_2(x_1, x_2, ..., x_n) = 1;\ \dots ;\ f_m(x_1, x_2, ..., x_n) = 1. \right\} \quad (11)$$

Дана система логических уравнений типа (11). Алгоритм поиска решений максимальных совместных подсистем системы включает следующие этапы: 1) вычисление представления значений выражений; 2) формирование максимальных совместных подсистем с использованием вышеуказанного алгоритма. Проведен анализ совместимости каждой (12) подсистемы:

$$\left\{ f_{j_1}(x_1, ..., x_n) = 1;\ f_{j_2}(x_1, ..., x_n) = 1; ...;\ f_{j_\kappa}(x_1, ..., x_n) = 1. \right\} \quad (12)$$

Проверено, является ли значение уникальным: $\prod_{i=1}^{\kappa} \Delta f_{j_i} = \tilde{0}$. Обосновано, если оно будет считаться уникальным, то рассматриваемая подсистема не будет общей; 3) вычисление логического умножения образов значений всех максимальных совместных подсистем; 4) формирование представления всех значений в *M* наборе.

Рассмотрено решение системы логических уравнений, основанное на аналитическом преобразовании логических выражений. Выявлено, что алгоритм включает следующие этапы. 1) передача через формулы в базисе D^1 д.н.ф. выражения (11) в уравнениях системы; 2) построение максимальных совместных подсистем системы с использованием A_M алгоритма на основе (12), анализ совместимости данной подсистемы, проверка того, что часть системы имеет решение; 3) удаление равносильных уравнений; 4) из максимальных совместных подсистем системы уравнений (11) вида (12) возможен переход к уравнению (13) с использованием алгоритма умножения функций алгебры логики, заданный в виде д.н.ф.:

$$\prod_{i=1}^{\kappa} \Delta f_{j_i} = 1 \quad (13)$$

В параграфе 2.2 решены задачи формирования аналитических выражений на разных базисах и перехода от одного к другому, доказаны теоремы преобразования функций в логической алгебре из одного базиса в другой.

1-я теорема. Логическая функция, состоящая из последовательности операций импликации $\xrightarrow[i=1]{n} A_i$, может быть записана в виде следующего выражения:

$$\xrightarrow[i=1]{n} A_i = \begin{cases} \bigwedge\limits_{i=1}^{n/2} \overline{A}_{2i-1} \vee \bigvee\limits_{j=1}^{(n/2)-1} \left(A_{2j} \bigwedge\limits_{i=j}^{(n/2)-1} \overline{A}_{2i+1} \right) \vee A_n, \text{ если } n = 2k; \\ \bigvee\limits_{j=1}^{(n/2)-1} \left(A_{2i-1} \bigwedge\limits_{i=j}^{(n/2)-1} \overline{A}_{2i} \right) \vee A_n, \text{ если } n = 2k+1, \end{cases} \quad (14)$$

2-я теорема. Логические функции, состоящие из последовательности операций штриха Шеффера $\overset{n}{\diagup\!\!\diagup}_{i=1} A_i$, представлены следующими как д.н.ф. в системе $\mathfrak{H}_1 = \{x_1 \wedge x_2, x_1 \vee x_2, \neg x\}$ в виде

$$\overset{n}{\diagup\!\!\diagup}_{i=1} A_i = \begin{cases} \overline{A}_1 \bigwedge\limits_{i=1}^{(n/2)-1} A_{2i+1} \bigvee\limits_{j=1}^{(n/2)-1} \left(\overline{A}_{2j} \bigwedge\limits_{i=j}^{(n/2)-1} A_{2i+1} \right) \vee \overline{A}_n, \text{ если } n = 2k; \\ A_1 \bigwedge\limits_{i=1}^{(n-1)/2} A_{2i} \vee \bigvee\limits_{j=2}^{(n-1)/2} \left(\overline{A}_{2j-1} \bigwedge\limits_{i=j}^{(n-1)/2} A_{2i} \right) \vee \overline{A}_n, \text{ если } n = 2k+1, \end{cases} \quad (15)$$

3-я теорема. Показано, что если операция «~»($\leftrightarrow$) в выражении эквивалентности является последовательной и нечетной, ее можно заменить операцией XOR. Если это четное число, необходимо ввести операцию отрицания перед общей формулой. Теорема может быть выражена в виде следующей формулы:

$$\underset{i=1}{\overset{n}{\sim}} A_i = \left\{ \sum_{i=1}^{n} A_i, \text{ если } n = 2k+1; \quad \neg\left(\sum_{i=1}^{n} A_i \right), \text{ если } n = 2k \right\}. \quad (16)$$

4-я теорема. Установлено, что последовательность логических выражений, состоящая из операции штриха Шеффера, выражается равномерно, как в системе $\{\wedge, +, 1\}$:

$$\overset{n}{\diagup\!\!\diagup}_{i=1} A_i = \bigwedge_{i=1}^{n} A_i + \sum_{i=3}^{n} \left(\bigwedge_{j=i}^{n} A_i \right) + 1. \quad (17)$$

В параграфе 2.3 приведены оценки сложности алгоритма решения системы булевых уравнений по формуле

$$\left\{ \mathfrak{A}_{11} \vee \ldots \vee \mathfrak{A}_{1t_1} = 1; \cdots; \mathfrak{A}_{m1} \vee \ldots \vee \mathfrak{A}_{mt_m} = 1. \right\} \quad . \quad (18)$$

Здесь $\mathfrak{A}_{ij}, i = \overline{1,t}, j = \overline{1,\rho_i}$, элементарные коньюнкции.

Алгоритм А, применение которого предусматривается во всех возможных случаях для решения системы уравнений, удовлетворяет оценке $\Psi_A \le \prod_{i=1}^{m} t_i$ сложности. Если он выражается через $D_i^0 = \mathfrak{A}_{i1} \vee \ldots \vee \mathfrak{A}_{it_i}$, ортогональных д.н.ф. и D_1 совершенной д.н.ф. удовлетворяют оценке $\Psi_{A_1} \le 2^n \sum_{i=2}^{m} t_i'$ сложности решения системы уравнений. Если система уравнений (18) состоит из кратчайшей д.н.ф., сложность решения системы уравнений определяется по формуле (здесь $\delta'(n) \to 0$ да $n \to 0$).

$$\Psi \le (m-1)\frac{2^{2n-2}}{\left(\log_2^2 n\right)\left(\log_2 \log_2 n\right)^2}\left(1+\delta'(n)\right) \quad (19)$$

Если система уравнений (18) состоит из сокращенной д.н.ф., сложность решения системы уравнений определяется по формуле
($L_i \sim 2^n n^{\log_2 \log_2 n}$, $\left|S_1\left(\mathfrak{A}, D_j\right)\right| \sim n^{\log_2 \log_2 n}$, $\left|N_{\mathfrak{A}}\right| \sim \log_2 n$ здесь $\delta(n) \to 0$, $n \to 0$).

$$\Psi \le (m-1) n^{2\log_2 \log_2 n} 2^{2n}\left(1+\delta(n)\right) \quad (20)$$

В параграфе 2.4 алгебраическая нелинейность может быть уменьшена при применении группировки в оптимизации полинома Жегалкина. В этом случае уравнение записывается в виде

$$A + A = 0; A \wedge 1 = A; A \wedge A = A; A \wedge 0 = 0; A \wedge B = B \wedge A. \quad (21)$$

Тогда функция с использованием равенств (Здесь $\deg(F) > \deg(G_i)$ ($i = \overline{1,k}$)).

$$F\left(x_0, x_1, \ldots, x_n\right) = G_1(x_0, x_1, \ldots, x_n) \wedge \cdots \wedge G_k(x_0, x_1, \ldots, x_n) = \prod_{i=0}^{k} G_i(x_0, x_1, \ldots, x_n). \quad (22)$$

Число элементарных конъюнкций можно уменьшить, введя операцию отрицания в булевую функцию, заданную в полиноме Жегалкина, но алгебраическая нелинейность функции увеличивается: $F(x)+1 = \left(F(x)\right)'$, $F(x)G(x) + F(x) = F(x)\left(G(x)+1\right) = F(x)\left(G(x)\right)'$. Можно ввести операцию отрицания в полином Жегалкина через формулы равной силы. Полученный полином получил название обобщенного полинома Жегалкина.

В третьей главе под названием **«Оценка отображений в процессах шифрования и их программное обеспечение»** проанализированы программное обеспечение для оценки отображений в стандартах шифрования также д.н.ф. и программа решения системы булевых уравнений, заданной в полиноме Жегалкина, блок-схемы и оценки сложности. В главе рассмотрены современные алгоритмы шифрования в зависимости от оптимизированных булевых формул передачи последовательности микрокоманд стандартного алгоритма шифрования ГОСТ Р34.12-2015(Кузнечик) на микроконтроллеры. Проведен также алгебраический криптоанализ стандартных симметричных алгоритмов шифрования AES и ГОСТ Р34.12-2015 (Кузнечик) на основе оптимизированных моделей, приведенных в первой и второй главах.

В параграфе 3.1 определены граф-схемы алгоритмов, матричный алгоритм для алгоритма шифрования Кузнечик и на их основе найдены минимальные д.н.ф. булевых функций микрокоманд в алгоритмах. Рассмотрены отображения *X*, *S*, *L* в алгоритме симметричного шифрования Кузнечик. Определен *X* в виде $\{Y_0 = Y_1; Y_1 = Y_2; Y_2 = x_1 Y_2 \vee \overline{x}_1 Y_K\}$ аналитической формы матричной схемы микрокоманд алгоритма отображения и как д.н.ф. булевой функции $\{Y_0 = 1; Y_1 = 1; Y_2 = 1; Y_K = \overline{x}_1;\}$.

Определено S в виде $Y_0 = Y_1;\ Y_1 = Y_2; Y_2 = x_1 Y_2 \vee \overline{x}_1 Y_3;\ Y_3 = Y_к$ аналитической формы матричной схемы микрокоманд алгоритма отображения и как форма булевой функции $\{Y_0 = 1; Y_1 = 1; Y_2 = 1; Y_3 = \overline{x}_1; Y_к = \overline{x}_1;\}$. Определено L в виде $\{Y_0 = Y_1; Y_1 = Y_2;\ Y_2 = \overline{x}_1 x_2 Y_3 \vee \overline{\overline{x_1}\,\overline{x_2}} Y_4; Y_3 = \overline{x}_3 Y_1 \vee Y_4; Y_4 = Y_5\}$ аналитической формы матричной схемы микрокоманд алгоритма отображения и как форма булевой функции $\{Y_0 = 1; Y_1 = 1; Y_2 = 1; Y_3 = \overline{x}_1; Y_4 = \overline{x}_1; Y_5 = \overline{x}_1; Y_6 = \overline{x}_1 \overline{x}_2 \overline{x}_3;$ $Y_7 = \overline{x}_1 \overline{x}_2 \overline{x}_3; Y_8 = \overline{x}_1 \overline{x}_2 \overline{x}_3 \overline{x}_4;\ Y_K = \overline{x}_1 \overline{x}_2 \overline{x}_3 \overline{x}_4;\}$.

В параграфе. 3.2 дано описание программных продуктов, которые помогают в построении математической модели отображений *MixColumns*, *SubBytes* в алгоритме шифрования AES.

Программа для каждого из 8 бит, выходящих из обратных отображений *SubBytes* определяет функцию, заданную в виде д.н.ф., а.н.ф. и параметры общих криптографических требований (рис.1). Приведено описание программных продуктов, которые помогают в построении математических моделей отображений *S*, *L* в алгоритме шифрования Кузнечик.

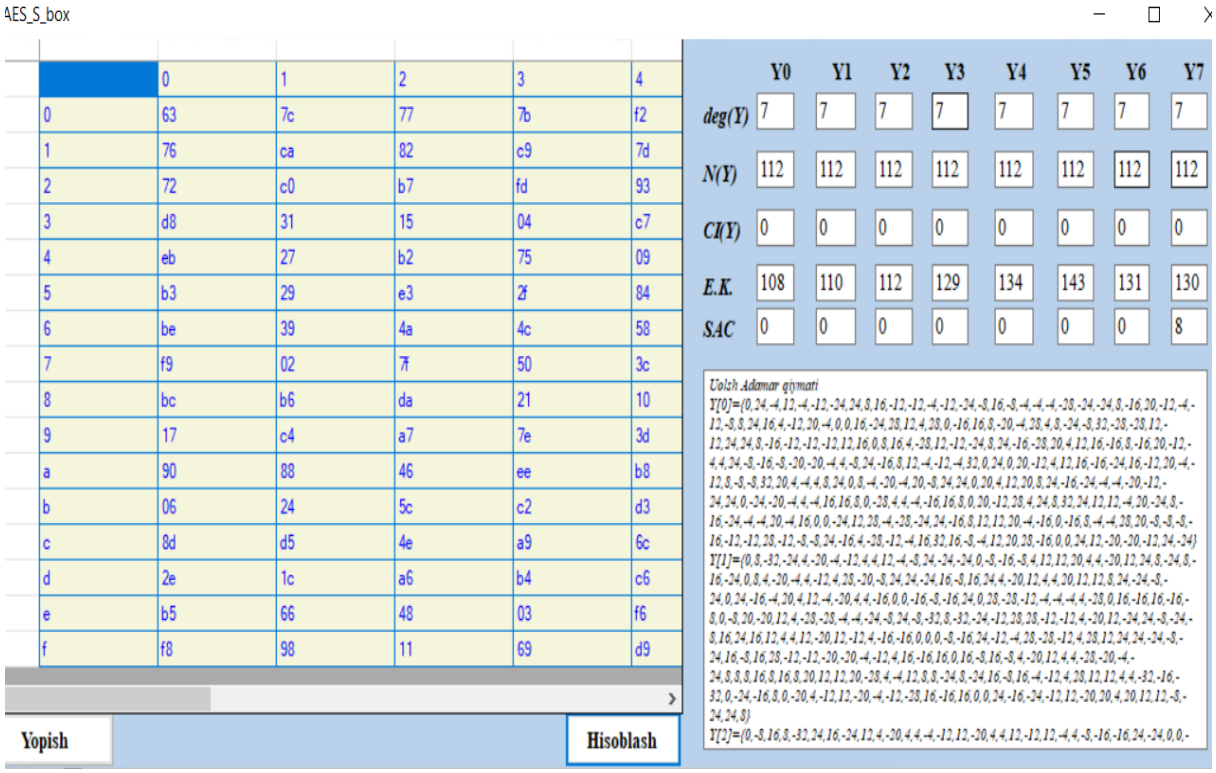


Рис. 1. Программное обеспечение для нелинейного отображения *SubBytes*

В параграфе 3.3 для полинома Жегалкина и д.н.ф. установлено, что теоретическая сложность алгоритма решения данной системы уравнений методом полного перебора равна $T = 4t + 2^n(4nt + 5t)$ экспоненциальной сложности.

Программа показывает алгебраическую нелинейность и время выполнения в системе уравнений. Обосновано, что теоретическая сложность алгоритмов минимизации Карты-Карно и Квайна булевых

функций системы уравнений в д.н.ф. равна $T = 5n^2/4 + 4nt + 3t$ полиномиальной сложности.

В параграфе 3.4 криптостойкость криптографических алгоритмов AES и Кузнечик оценены на основе метода алгебраического криптоанализа.

Доказана практическая устойчивость алгоритма шифрования к методу алгебраического криптоанализа на примере алгоритм AES: при количестве раундов 3 и выше в модели, заданной д.н.ф.; когда число раундов в модели, заданной в виде обобщенного полинома Жегалкина равно 6 и выше; когда число раундов в модели, заданной в виде обобщенного и сгруппированного полинома Жегалкина равно 5 и выше.

Алгоритм Кузнечик оказался неэффективным для использования в алгебраическом криптоанализе модели, заданной в д.н.ф. из-за создания 2^{46} новых переменных и уравнений в самом отображении L в модели в форме д.н.ф.. Когда число раундов в модели обобщенного полинома Жегалкина равно 6 и выше, когда число раундов в модели обобщенного и сгруппированного полинома Жегалкина равно 5 и выше, доказана практическая устойчивость алгоритма шифрования к методу алгебраического криптоанализа.

В модели обобщенного полинома Жегалкина образование дополнительных уравнений и неизвестных после каждого отображения представлено в табл. 4. Параметры системы уравнений, соответствующие числу раундов в алгоритме Кузнечик, приведены в табл. 5.

Параметры модели в обобщенном полиноме Жегалкина, представляющем отображения в алгоритме Кузнечик Таблица 4.

Отображения	Количество уравнений (КУ)	Количество неизвестных (КН)
X	256	256
S	5376	5376
L	128	128

Параметры системы уравнения в обобщенном полиноме Жегалкина, представляющем алгоритм Кузнечика Таблица 5

Раунды	Количество уравнений (КУ)	Количество уравнений		Сложность решения КУ	Память, необходимая для хранения КУ, байт
			в виде степени 2		
2	11520	11520	$2^{13,4918}$	$2^{40,4755}$	
6	34560	34560	$2^{15,0768}$	$2^{45,2304}$	2^{74}
10	60288	52096	$2^{15,6688}$	$2^{47,0066}$	

ЗАКЛЮЧЕНИЕ

1. Для современных алгоритмов симметричного шифрования приведены правила оценки алгоритмов шифрования на основе алгебраического криптоанализа по общим криптографическим требованиям.

2. На основе метода алгебраического криптоанализа разработаны оптимизированные математические модели алгоритмов симметричного шифрования ГОСТ Р34.12-2015, AES, A5/1 и дана оценка общим криптографическим требованиям.

3. Доказано, что отображение *L* в алгоритме шифрования ГОСТ Р34.12-2015 более эффективно, чем отображение *MixColums* в алгоритме шифрования AES, как следствие утверждений 1-4, в частности определены:

– зависимость каждого выходного бита от входящих значений бита минимум в **5,71** раза выше;

– зависимость каждого входного бита от выходящих значений бита минимум в **5,1** раза выше.

4. Решена задача нахождения системы максимальных подсистем систем логических уравнений. Предложен алгоритм нахождения максимального верхнего нуля монотонной логической функции. Разработана эффективная процедура вычисления значений монотонных функций *f* в *n*-мерных кубических наборах.

5. На основе поиска максимального верхнего нуля монотонных функций в логической алгебре разработан алгоритм решения и поиска максимальных совместных подсистем систем логических уравнений.

6. Решены задачи построения и трансформации аналитических выражений различных базисов, доказаны теоремы о выражении и преобразовании функций в логической алгебре в различных базисах.

7. Разработаны методы и алгоритмы оптимизации булевых функций в виде полинома Жегалкина. Определены этапы решения булевых уравнений в виде полинома Жегалкина.

8. Созданы оптимизированные булевые формулы при передаче последовательности микрокоманд алгоритма шифрования Кузнечика на микроконтроллеры.

9. Создано программное обеспечение, вычисляющее общие криптографические параметры отображений стандарта Кузнечик и AES-128.

10. Разработано программное обеспечение для решения систем булевых уравнений в базисе полинома Жегалкина и минимизированной д.н.ф.. Вычислено сложность решения системы булевых уравнений методом полного перебора.

11. Для алгоритмов шифрования Кузнечика и AES проведен алгебраический криптоанализ с использованием математических моделей, определенных в разных базисах. В соответствии с проведенным анализом

доказана практическая устойчивость метода алгебраического криптоанализа для алгоритмов шифрования Кузнечик и AES с числом раундов 6 и выше.

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

NATIONAL UNIVERSITY OF UZBEKISTAN

BERDIMURODOV MANSUR ALISHEROVICH

LOGICAL METHODS FOR SOLVING PROBLEMS OF CRYPTANALYSIS

05.01.05 – Methods and systems of information protection. Information security (Physical and mathematical sciences)

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

Tashkent-2023

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number №B2020.4.PhD/FM553.

Dissertation has been prepared at National University of Uzbekistan.

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

Scientific superviser:	**Kabulov Anvar Vasilovich** Doctor of Technical Sciences, Professor
Official opponents:	**Abduraximov Baxtiyor Fayziyevich** Doctor of Physical and Mathematical Sciences, Professor
	Saidov Abdusobir Abduraxmonovich Doctor of Technical Sciences, Professor
Leading organization:	**"UNICON.UZ" STATE UNITARY ENTERPRISE**

Defense will take place «____» _____2023 at _____ at 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 is possible to review in Information-resource centre at National University of Uzbekistan (is registered №____) (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Ph.: (+99871) 246-02-24).

Abstract of dissertation sent out on «____» _____2023 year

(Mailing report № _____on «____» _____2023 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.

G.U. Juraev
Deputy Chairman of Scientific Seminar under Scientific Council on award of scientific degrees, D.F.-M.S.

INTRODUCTION (abstract of PhD thesis)

The aim of the research work is the analysis of mappings and their tolerance in cryptographic encryption algorithms AES and GOST R34.12-2015 (Kuznechik), evaluation using the algebraic method of cryptanalysis, as well as the creation and evaluation of the complexity of a mathematical model on various grounds using logical methods.

The research objective are cryptographic algorithms, mathematical mapping models, a system of Boolean equations, Boolean functions, microcommand forms of algorithms.

Scientific novelty of research work is as follows:

optimized mathematical models were created based on the methods of algebraic cryptanalysis of AES algorithms, GOST R34.12-2015 (Kuznechik), A5/1;

an assessment of the general cryptographic requirements of modern symmetric encryption algorithms AES, GOST R34.12-2015 (Kuznechik) was calculated based on their mathematical models and algebraic cryptanalysis was carried out based on various logical bases of algorithms

optimized formulas for Boolean functions were created when transferring a sequence of microcommands to microcontrollers of the Kuznechik encryption algorithm;

criteria and algorithms for converting mappings in symmetric encryption algorithms AES, GOST R34.12-2015 (Kuznechik) and A5/1 to Boolean functions given in different bases were developed, and a theorem for transforming logical formulas from one basis to another was proved;

algorithms for solving systems of Boolean equations based on the search for the maximum upper zero of monotone Boolean functions have been developed and their complexity has been estimated.

Implementation of the research results. Based on optimized mathematical models created for modern encryption algorithms AES, Kuznechik, A5/1, and the results obtained from the evaluation of general cryptographic requirements:

An optimized mathematical model of AES encryption algorithms, Kuznechik and the results of an assessment of general cryptographic requirements are used in the project OT-Atex-2018-486 “Implementation of logical control and information protection systems based on programmable logic controllers and an automated CAD logic system for their design” when analyzing and optimizing forms (Reference 04/10-2807 dated May 17, 2022 of the National University of Uzbekistan named after Mirzo Ulugbek). The application of scientific results made it possible to optimally implement and analyze encryption algorithms based on a microcontroller.

the rules for evaluating encryption algorithms for modern symmetric encryption algorithms for compliance with general cryptographic requirements are used in the process of evaluating cryptographic algorithms using modern cryptanalysis methods within the framework of the project “Creating

Cryptographic Algorithms" held at UNICON.UZ SUE. Also, the data obtained from the decisions of applying criteria and algorithms for reducing to Boolean functions in different bases of mappings in the GOST R34.12-2015 symmetric block cipher algorithm were used in UNICON.UZ SUE when assessing the stability of symmetric block cipher algorithms used in national secure systems (Reference 04/10-2807 dated May 17, 2022 of the National University of Uzbekistan named after Mirzo Ulugbek). The application of scientific results made it possible to evaluate and analyze the stability of symmetric block cipher algorithms used in national security systems.

The structure and volume of the thesis: The dissertation work consists of an introduction, three chapters, a conclusion, a list of references and an appendix. The volume of the dissertation is 114 pages.

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

I бўлим (1 часть; part 1)

1. Kabulov A.V., Ashurov A., **Berdimurodov M.A.** “Analytical transformations in minimizing logical functions”. International Conference on Information Science and Communications Technologies ICISCT 2020 Applications, Trends and Opportunities. (№3 Scopus IF=0.4).
2. Kabulov A.V., **Berdimurodov M.A.**, Saymanov I.M. “Kriptografik algoritm mikrobuyruqlarining mantiqiy bul funksiya shakli (AES, El-Gamal)”. Samarqand davlat universiteti ilmiy axborotnomasi. №3(2021), 90-100 b. (01.00.00 №2)
3. А.В. Кабулов, Э.Урунбаев, **Бердимуродов М.А.**, “Логический метод нахождения максимальных совместних подсистем систем булевых уравнений”. Samarqand davlat universiteti ilmiy axborotnomasi. №5(2020), 4-15 b. (01.00.00 №2)
4. **Berdimurodov M.A.** “AES shifrlash algoritm tahlili” // Informatika va energetika muammolari №6(2021), 37-44 b. (05.00.00 №5)
5. Kabulov A. V., **Berdimurodov M.A.** “Parametric algorithm for searching the mini-mum lower unity of monotone boolean func-tions in the process synthesis of control automates” // International conference on information science and communications technologies: applications, trends and opportunities ICISCT 2021 (№3 Scopus IF=0.1)
6. Kabulov A. V., Saymanov I., **Berdimurodov M.A.** “Minimum logical representation of microcommands of cryptographic algorithms (AES)” // International conference on information science and communications technologies: applications, trends and opportunities ICISCT 2021 (№3 Scopus IF=0.1)
7. Kabulov A. V., **Berdimurodov M.A.** “Optimal representation in the form of logical functions of microinstructions of cryptographic algorithms (RSA, El-Gamal)” // International conference on information science and communications technologies: applications, trends and opportunities ICISCT 2021 (№3 Scopus IF=0.1)
8. Байжуманов А.А., **Бердимуродов М.А.**, Мухаммадиев Ф.Р. “Оптималлаштирилганьный метод решения некоторых классов систем нелинейных уравнений второй степени, основанный на преобразовании многочленов” Мухаммад ал-Хоразмий авлодлари, № 4 (22), декабр 2022, 154-157 стр. (05.00.00 №10)

II бўлим (2 часть; part 2)

1. **Berdimurodov M.A.**, Farmonov B.D. “AES kriptografik algoritmning bul tenglamalar sistemasi” // Международный научно-практический

конференция «Современные проблемы прикладной математики и информационных технологий» БухДУ. 2021. – с. 86.

2. **Berdimurodov M.A.**, Xudoyqulov K.T. “AES, El-Gamal kriptografik algoritmlarining graf sxema algoritmi asosida bul funksiyasi” // Международный научно-практический конференция «Современные проблемы прикладной математики и информационных технологий» БухДУ. 2021. – с. 82-83.

3. **Berdimurodov M.A.** “GOST R34.12-2015(Kuznechik) shifrlash algoritmini tahlili” // Institute of Mathematics named after V.I. Romanovskiy at the AS of Uzbekistan Bukhara branch of the Institute of Mathematics ABSTRACTS of the Republican Scientific Conference with the participation of foreign scientists DIFFERENTIAL EQUATIONS AND RELATED PROBLEMS OF ANALYSIS Bukhara, Uzbekistan, November 04–05, 2021(295-296 p.)

4. Kabulov A., **Berdimurodov M.A.** “On the existence of majorant algorithms over control systems” // The VII International Scientific Conference Conference Modern Problems of Applied Mathematics and Information Technologies Al-Khwarizmi 2021 15-17 November, 2021, Fergana, Uzbekistan (232 p.)

5. Kabulov A.V., **Berdimurodov M.A.** “GOST R 34.12-2015 (Kuznyechik) analysis of a cryptographic algoritm” // The VII International Scientific Conference Conference Modern Problems of Applied Mathematics and Information Technologies Al-Khwarizmi 2021 15-17 November, 2021, Fergana, Uzbekistan (21 p.)

6. **Berdimurodov M.A.**, Isoqov G‘.S. “Kuznechik shifrlash algoritmidagi *L* chiziqli akslantirish tahlili” // Matematik fizika va matematik modellashtirishning zamonaviy muammolari: Xalqaro ilmiy konferensiya materiallari (3–4 Dekabr 2021, Qarshi, O‘zbekiston).–Qarshi. 2021. (160-161 bet)

7. **Berdimurodov M.A.**, Bozorov O.N. “Hamming masofasi va kodi axborot xavfsizligida” // – Matematik fizika va matematik modellashtirishning zamonaviy muammolari: Xalqaro ilmiy konferensiya materiallari (3–4 Dekabr 2021, Qarshi, O‘zbekiston).– Qarshi. 2021. (196-197 bet)

8. **Berdimurodov M.A.** “Ixtiyoriy bul funksiyasini Jegalkin ko‘phad ko‘rinishini” // Tadqiqot.uz da “O‘zbekistonda ilmiy- amaliy tadqiqotlar” mavzusida Respublika 18-ko‘p tarmoqli ilmiy masofaviy onlayn konferensiya, 2020 yil. Toshkent. // 259-260-b.

9. **Berdimurodov M.A.**, Tursunov S. “AES kriptografik algoritmning S-blokini bul funksiya ko‘rinishi” // Namangan davlat universitetida “O‘zbekiston yoshlarida axborot madaniyatini shakllantirishni dolzarb muammolari” mavzusida o‘tkaziladigan Respublika ilmiy-amaliy anjumani Namangan - 2021. 83-85 bet.

10. **Berdimurodov M.A.**, Farmonov B.D. “Mantiqiy funksiyalarni minimallashtirish usullari (Karta Karno, Kvain-Mak-sinf)” // Berdaq nomidagi Qoraqalpoq Davlat universiteti «Tabiiy fanlarni rivojlantirishda axborot-kommunikatsiya texnologiyalarining o‘rni» Respublika ilmiy-amaliy konferensiyasi maqolalar to‘plami 9-noyabr, 2021-yil. (208-209 bet)

11. Kabulov A.V., **Berdimurodov M.A.** Gost R34.12-2015 (Kuznechik) kriptografik algoritmidagi *L* chiziqli akslantirishning Bul funksiya shakli. 10.09.2021y., № DGU 12633, O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk agentligi.

12. **Berdimurodov M.A.**, Saymanov I.M. AES(Rijndael) kriptografik algoritmidagi S chiziqsiz akslantirishning Bul funksiya shakli. 10.09.2021y., № DGU 12634, O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk agentligi.

13. **Berdimurodov M.A.**, Xudoyqulov K.T., Boltaev Sh.T. Jegalkin ko‘phadida berilgan mantiqiy tenglamalar tizimini yechish dasturi. 17.02.2022y., № DGU 14999, O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk agentligi.

14. Kabulov A.V., **Berdimurodov M.A.**, Muxamadiev F.R., Farmonov B.D. Dizyunktiv normal shakldagi mantiqiy tenglamalar tizimini yechish dasturi. 17.02.2022y., № DGU 14998, O‘zbekiston Respublikasi Adliya vazirligi huzuridagi Intellektual mulk agentligi.

Avtoreferat O‘zbekiston Milliy universitetining “O‘zMU xabarlari” jurnali tahririyatida tahrirdan o‘tkazildi va o‘zbek, ingliz, rus tillaridagi matnlarning mosligi tekshirildi.

Bosmaxona litsenziya:

Bosishga ruxsat etildi 23.03.2023. Hajmi 3,5 bosma taboq.
Bichimi 84×60 1/16. Adadi 100 nusxa. Buyurtma 88.

«NUR ALLABAMA» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: Toshkent sh., Almazar ko‘chasi 6/7.