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

O‘ZBEKISTON MILLIY UNIVERSITETI

BOZOROV ASQAR XAITMUROTOVICH

BARDOSHLI KRIPTOGRAFIK KALITLARNI ISHLAB CHIQISH

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

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

Toshkent – 2025

UO‘K: 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

BOZOROV ASQAR XAITMUROTOVICH

BARDOSHLI KRIPTOGRAFIK KALITLARNI ISHLAB CHIQISH

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

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

Toshkent – 2025

Fizika-matematika fanlari bo‘yicha falsafa doktori (Doctor of Philosophy) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida №B2022.3.PhD/FM774 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 (ik-fizmat.nuu.uz/) va “ZiyoNet” Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Jurayev Gayrat Umarovich** fizika-matematika fanlari doktori, professor
Rasmiy opponentlar:	**Kabulov Anvar Vasilovich** texnika fanlari doktori, professor
	Sattarov Alijon Bozorboyevich fizika-matematika fanlari bo’yicha PhD
Yetakchi tashkilot:	**UNICON.UZ MChJ**

Dissertatsiya himoyasi O‘zbekiston Milliy universiteti huzuridagi DSc.03/30.12.2019.FM.01.02 raqamli Ilmiy kengashning “07” 11 2025-yil soat 16⁰⁰ 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 (174 raqami bilan ro‘yxatga olingan). Manzil: 100174, Toshkent sh., Olmazor tumani, Universitet ko‘chasi, 4-uy. Tel.: (+99871) 246-02-24.

Dissertatsiya avtoreferati 2025-yil “25” oktyabr kuni tarqatildi.
(2025-yil “19” 09 dagi 1 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., professor

B.F. Abduraximov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, f.-m.f.d., professor

KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon miqyosida olib borilayotgan ko‘plab ilmiy va amaliy tadqiqotlarda shifrlash algoritmlarida mustahkam va xavfsiz kalitlarni ishlab chiqishga katta e’tibor qaratilmoqda. Bunda, bardoshli kriptografik kalitlarni ishlab chiqish, ularning tasodifiylik xususiyatlarini takomillashtirish va kalit tahlillariga nisbatan bardoshliligini oshirish muhim ahamiyat kasb etadi. Axborotlarni himoyalashning kriptografik algoritmlari, simmetrik shifrlash algoritmlari, xesh funksiyalar, elektron raqamli imzo algoritmlarini yaratish, apparat, dasturiy vositalarni ishlab chiqish axborot xavfsizligi va kriptologiya sohasining tadqiqot obyekti hisoblanadi. Shu sababli, zamonaviy kriptografik talablarga javob beruvchi, yuqori entropiyaga ega bardoshli kalitlarni yaratish kriptografiyaning muhim vazifalaridan biri bo‘lib qolmoqda.

Hozirgi kunda dunyoda kompyuter tizimlarida axborotlarning maxfiyligi va konfidensialligini ta’minlash uchun kriptografik tizimlar keng qo‘llanilmoqda. Bunday tizimlarning bevosita xavfsizligi unda qo‘llaniladigan shifrlash algoritmining bardoshliligi va kalitning maxfiyligi bilan chambarchas bog‘liqdir. Shifrlash kaliti, odatda, tasodifiy bitlar ketma-ketligi bo‘lib, ular psevdotasodifiy sonlar generatori (PRNG) yoki oqimli shifrlash algoritmlari yordamida yaratiladi. Generatsiya qilingan ketma-ketliklar yuqori darajada tasodifiylikka ega bo‘lishi, statistik testlardan muvaffaqiyatli o‘tishi hamda boshlang‘ich yoki joriy holatining bir qismi kriptotahlili ma’lum bo‘lganda ham bashorat qilaolmasligi lozim. Shuning uchun zamonaviy axborot xavfsizligi tizimlarida tasodifiylik darajasi yuqori bo‘lgan ketma-ketliklarni generatsiyalash algoritmlarini ishlab chiqish hamda shifrlashda bardoshli kriptografik kalitlardan foydalanish dolzarb ilmiy-texnik muammolardan biri bo‘lib qolmoqda. Shu sababli bardoshli kriptografik tejamkor algoritmlarini ishlab chiqish hamda ularning samarodarligini aniqlash maqsadli ilmiy tadqiqotlardan hisoblanadi.

Mamlakatimizda axborot texnologiyalari, axborot xavfsizligi va uning kriptografik himoyasi sohalarida ilmiy va amaliy tadqiqotlarga alohida e’tibor qaratilmoqda. Bardoshli kriptografik kalitlarning samarali usullarini ishlab chiqish, ularni amaliyotda qo‘llash va umumlashtirish qobiliyatini oshirish bugungi kunda dolzarb masalalardan biri hisoblanadi. So‘nggi yillarda olib borilgan izlanishlar natijasida kriptografik algoritmlarni tahlil qilish usullari va baholash kriteriyalari takomillashib, axborotni kriptografik himoyalashning milliy tizimini yanada rivojlantirish yo‘lida muhim natijalarga erishildi. Milliy kriptologiya sohasini rivojlantirishning dolzarb yo‘nalishlari bo‘yicha psevdotasodifiy sonlar generatorlarini yaratishga alohida e’tibor qaratilmoqda [1] . Qaror ijrosini ta’minlashda simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini ishlab chiqish hamda yengil vaznli oqimli shifrlash algoritmlarini yaratish va ulardan

[1] O‘zbekiston Respublikasi Prezidentining 15.08.2024 yildagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-son qarori

psevdotasodifiy sonlar generatori sifatida foydalanib, bardoshli kalitlarni generatsiya qilish masalalari tadqiq qilish muhim ahamiyatga ega.

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

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

Muammoning o‘rganilganlik darajasi. Axborot xavfsizligining kriptografik himoyasi, bardoshli kriptografik kalitlarni generatsiya qiladigan algoritmlarni yaratish, ularni kriptotahlil usullariga baholash bo‘yicha B.Shnayer, N.Ferguson, G.Vernam, T.Zigentaler, A.O.Kerkxoffs, D.Ye.Knut, K.Ye.Shennon, M.B.Budko, I.I.Slepovichev kabi olimlar tomonidan tadqiqotlar olib borilgan. So‘nggi bir necha yil ichida ushbu mualliflar tomonidan nazariy va amaliy nuqtai nazaridan axborotlarni himoyalash va algoritmlash masalalari bo‘yicha ko‘plab ishlar amalga oshirilgan. Shifrlash algoritmlarining apparat va apparat-dasturiy vositalarini ishlab chiqish bo‘yicha AQSHda « CRYSTALS-Kyber», Rossiya Federatsiyasida «Ankad», Fransiyada «Thales Group» kabi kompaniyalar tomonidan muhandislik-tadqiqot ishlari olib borilmoqda.

Respublikamizda M.M.Aripov, B.F.Abdurahimov, S.K.Ganiev, D.Ye.Akbarov, A.V.Kabulov, O.P.Axmedova, G.U.Jurayev, G.N.Tuychiyev, D.M.Kuryazov, A.I.Ikramov, Z.T.Xudoyqulov, I.R.Rahmatullayev kabi tadqiqotchilar tomonidan axborotni himoyalashning kriptografik algoritmlari, simmetrik shifrlash algoritmlari, xesh funksiyalar, elektron raqamli imzo algoritmlarini yaratish, apparat, dasturiy vositalarni ishlab chiqishga oid ilmiy tadqiqotlar olib borilgan. Lekin, hozirgi kunda respublikamizda kriptografik ehtiyojlar uchun psevdotasodifiy sonlar generatorlarini tadqiq qilish, shuningdek, yengil vaznli kriptografik algoritmlar ishlab chiqish masalalari bo’yicha yetarlicha ilmiy-tadqiqot ishlari olib borilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti ilmiy-tadqiqot rejasiga muvofiq Uzb-Ind-2021-98 “Oqimli shifrlash algoritmlarini tadqiq qilish va ishlab chiqish” mavzusidagi amaliy loyihasi doirasida bajarilgan.

Tadqiqotning maqsadi kriptografik talablarga javob beruvchi, tasodifiylik darajasi yuqori bo‘lgan bardoshli kriptografik kalitlarni ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini generatsiya qilish algoritmini ishlab chiqish;

dasturiy ko‘rinishda amalga oshirishga qulay bo‘lgan, yengil vaznli oqimli shifrlash algoritmini ishlab chiqish;

apparatda amalga oshirishga qulay bo‘lgan, yengil vaznli oqimli shifrlash algoritmini ishlab chiqish;

ishlab chiqilgan shifrlash algoritmlari generatorlarining tasodifiylik darajasini baholash;

ishlab chiqilgan shifrlash algoritmlari kalit generatorlari bardoshligini kriptotahlil usullari yordamida baholash;

ishlab chiqilgan oqimli shifrlash algoritmlari kalit generatorlarini tezlik va amalga oshirish xususiyatlari bo‘yicha taqqoslash.

Tadqiqotning ob’yekti sifatida kriftografik kalit sifatida foydalanish mumkin bo‘lgan, tasodifiylik darajasi yuqori bo‘lgan psevdotasodifiy ketma-ketliklardan iborat.

Tadqiqotning predmeti psevdotasodifiy ketma-ketliklarni generatsiya qilish imkonini beruvchi apparat va dasturiy ko‘rinishda amalga oshirishga mo‘ljallangan oqimli shifrlash algoritmlari va ularni kriptografik xususiyatlarini baholash usullaridan iborat.

Tadqiqotning usullari. Tadqiqot jarayonida kriptografiya va kriptotahlil usullari, diskret matematika, ehtimollar nazariyasi, sonlar nazariyasi va kriptografiyaning matematik asoslaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

simmetrik blokli shifrlash algoritmlari uchun kriptotahlil usullariga bardoshli bo’lgan, raund kalitlarini generatsiya qilish algoritmi ishlab chiqilgan;

ichki holat massivlarini aralashtirishga asoslangan, dasturiy amalga oshirish qulay bo’lgan oqimli shifrlash algoritmi ishlab chiqilgan;

chiziqsiz teskari aloqali siljitish registrlariga asoslangan, apparatda amalga oshirishga mo’ljallangan, umumiy uzunligi 128 bit bo‘lgan hamda 3 ta siljitish registrlaridan iborat oqimli shifrlash algoritmi ishlab chiqilgan;

yuqori darajadagi tasodifiylikni ta’minlaydigan kriptografik psevdotasodifiy sonlar generatorining gibrid modeli ishlab chiqilgan;

ishlab chiqilgan kalitlarni generatsiya qiladigan algoritmlar kriptotahlil usullari yordamida baholangan va 2^{100} dan ortiq iteratsiyalarda hujumlarga bardoshli ekanligi isbotlangan;

ishlab chiqilgan oqimli shifrlash algoritmlari amalga oshirish tezligi bo‘yicha taqqoslangan hamda ularning kriptografik xavfsizligi statistik testlar orqali baholangan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

dasturiy ko‘rinishda amalga oshirishga qulay oqimli shifrlash algoritmining dasturiy vositasi ishlab chiqilgan;

LFSR (chiziqli teskari aloqali siljitish registri) registrlariga asoslangan oqimli shifrlash algoritmini apparatda amalga oshirish sxemasi va dasturiy vositasi ishlab chiqilgan.

Tadqiqot natijalarining ishonchliligi dissertatsiyada olingan natijalarning ishonchliligi undagi matematik mulohazalarning qat'iyligi, o‘tkazilgan sonli tadqiqot natijalari bilan tasdiqlanganligi hamda kriptografik algoritmlarni kriptotahlillash usullaridan olingan real hamda tajribaviy natijalar bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini generatsiya qilish, apparat va dasturiy amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmlarida kalitni generatsiyalash algoritmlari kriptografik himoyalash vositalarini yaratishda foydalanish mumkinligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati oqimli shifrlash algoritmlari asosida kalitlarni generatsiya qilishga mo‘ljallangan apparat va dasturiy vositalarni yaratishga xizmat qiladi. Ular kompyuter tizimlari va tarmoqlarida ma'lumotlarning maxfiyligi hamda konfidensialligini ta'minlashda amaliy jihatdan muhim ahamiyatga ega bo‘lib, apparat va dasturiy shaklda qulay integratsiyalanishi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Taklif etilgan algoritmlar va ular asosida ishlab chiqilgan dasturiy vositalardan olingan natijalar bo‘yicha:

AAOOSHA80 (apparatda amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmi) asosida Axborot-kommunikatsiya texnologiyalari va aloqa harbiy institutida bardoshli kriptografik kalitlar ishlab chiqishda qo'llanilgan (O‘zbekiston Respublikasi Mudofa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy institutining 2024 yil 6 noyabrdagi 2648-son ma'lumotnomasi). Natijada, shifrlash va dastlabki matnga o‘girish vaqti bo‘yicha 13% samaradorlikka erishilgan.

Ichki holat massivlarini aralashtirishga asoslangan, dasturiy amalga oshirishga mo'ljallangan oqimli shifrlash algoritmidan Uzb-Ind-2021-98-«Oqimli shifrlash algoritmlarini tadqiq qilish va ishlab chiqish» mavzusidagi amaliy loyihada axborotni uzatishda uning maxfiyligini ta'minlash va uzatish jarayonidagi xatoliklar sonini kamaytirishda qo‘llanilgan (O‘zbekiston Milliy universitetining 2024 yil 16 dekabrdagi 04/11-13194-son ma'lumotnomasi). Ilmiy natijalar asosida ishlab chiqilgan dasturiy vosita yordamida axborotni uzatishda uning maxfiyligini ta'minlash va uzatish jarayonidagi xatoliklar sonini kamaytirishga erishilgan.

Tadqiqot natijalarining approbatsiyasi. Mazkur tadqiqot natijalari 5 ta ilmiy-amaliy anjumanlarda, jumladan, 2 ta xalqaro va 3 ta respublika ilmiy-amaliy anjumanlarda muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e'lon qilinganligi. Dissertatsiya mavzusi bo‘yicha jami 14 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish uchun tavsiya etilgan ilmiy nashrlarida 9 ta maqola, shundan, 4 tasi xorijiy va 5 tasi respublika jurnallarida nashr etilgan. Shuningdek, EHM uchun yaratilgan 2 ta dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 112 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

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

Dissertatsiyaning **«Kriptografik kalitlarni yaratishda psevdo tasodifiy sonlar generatorlaridan foydalanish»** deb nomlangan birinchi bobida psevdotasodifiy sonlar generatorlari yordamida simmetrik blokli shifrlash algoritmlari uchun raund kalitlarni generatsiyalash masalalarini yechish bo‘yicha tavsiyalar, shuningdek dasturiy va apparat ko‘rinishda amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmlarida masalalar va ulardagi muammolar hamda ularni yechimlari muhokama qilingan.

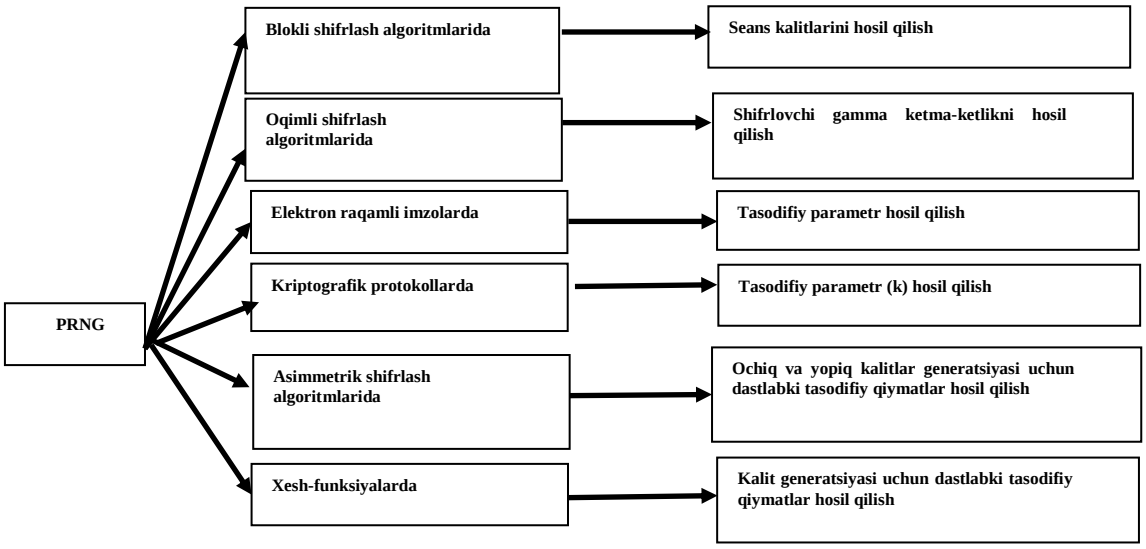
§1.1-paragrafda tasodifiy ketma-ketliklar va ularning xususiyatlari tahlil qilingan. Kriptografik tizimlarning bardoshligi unda foydalanilgan algoritm va kalitning bardoshligi bilan belgilanadi. Kriptografik algoritmlar bardoshli bo‘lgan taqdirda ham, zaif kalitdan foydalanilganda axborotning himoyalanganlik darajasi yuqori bo‘lmaydi. Kerkxoffs tamoyili asosida kriptografik tizimning xavfsizligi faqatgina maxfiy kalitga bog‘liq bo‘lishi kerak, algoritm yoki shifrlash usuli ochiq bo‘lishi kerak. Shuningdek, kalitning bardoshligi uni hosil qilgan tasodifiy ketma-ketliklarning tasodifiylik darajasiga bog‘liq. Xususan, tasodifiy sonlar yoki bitlar ketma-ketligini yaratish uchun tasodifiy sonlar generatorlari deb ataladigan qurilmalar qo‘llaniladi va shu asosidagi ma’lumotlar keltirib o‘tilgan. Tasodifiy generatorlarda entropiya tasodifiylik va xavfsizlikning asosiy o‘lchovi hisoblanadi.

Matematik jihatdan entropiya esa Shennon entropiyasi formulasi orqali ifodalanadi: $H(\mathrm{x}) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i)$ (1.1)

H(x)ning logarifm xususiyatlaridan foydalanib quydagicha formulaga ega bo‘ladi: $H(\mathrm{x}) = -\sum_{i=1}^{n} \frac{1}{n}(-\log_2 n) = \log_2 n$ (1.2)

Barcha natijalar bir xil ehtimollikka ega bo‘lsa, ya'ni eng maksimal tasodifiylik bo‘lsa, unda entropiya eng yuqori bo‘ladi. Shuningdek, entropiya yetarli bo‘lmasa**,** shifrlangan ma’lumotlar buzilishi mumkin. Tasodifiy sonlar kriptografiyaning asosiy omillaridan biri bo‘lib, ularning ishonchli generatsiyasi kriptografik xavfsizlikning asosi hisoblanadi. Kriptografiyada ishlatiladigan tasodifiy sonlar yuqori entropiyaga ega bo‘lishi va bashorat qilib bo‘lmaydigan bo‘lishi kerakligi tavsiflandi.

Kriptografik tizimlar maxfiy kalitdan foydalanib, yetarli katta davr uzunligiga ega va tasodifiylik darajasi yuqori bo‘lgan PRNG dan foydalanish maqsadga muvofiqdir. Shuningdek hozirgi kunda PRNG dan amalda ko‘plab kriptografik tizimlarda keng qo‘llanilishi 1-rasmda keltirib o’tilgan.



1-rasm. PRNGning qo‘llanish sohalari

Mazkur PRNGlar uchun kriptotahlil usullarini amalga oshirish ketma-ketligi o‘rganilgan hamda ushbu tahlil usullari shifrlash algoritmidagi qaysi zaiflikning mavjudligiga asoslanishi ko‘rsatilgan. Shuningdek, simmetrik shifrlash algoritmlari yordamida ishlab chiqilgan ketma-ketliklarni tasodifiylikka baholash testlari haqida ma’lumotlar keltirilgan. Psevdotasodifiy generator parametri $p, k, a_l, a_2, \dots\dots, a_k;\ x_{0,}, x_{-l}, \dots\dots, x_{-k+1}$. Boshlang‘ich qiymat $\mathrm{x}_0, \mathrm{x}_{-1}, \dots\dots, \mathrm{x}_{-\mathrm{k}+1} \in \mathrm{A}$ shunday ixtiyoriy tanlanadiki, 0 qiymatga bir vaqtda. $a_l, a_2, \dots\dots, a_k \in A$ rekurent koeffitsient shunday tanlanadiki, hosil qilingan ko‘phad quydagicha bo‘ladi:

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k \qquad (3)$$

1-teorema. Agar k bitli chiziqli teskari aloqali siljitish registri (LFSR) da foydalaniladigan ko'phad primitiv ko'phad bo'lsa, u holda uning davri $L = 2^k - 1$ - maksimal uzunlikga ega bo’ladi.

§1.3-paragrafda kriptografik xavfsiz psevdotasodifiy sonlar generatorlari (CSPRNG) shunday tasodifiy generatorlarki, ulardan olingan tasodifiy sonlarning bashorat qilib bo‘lmasligini kafolatlaydi. CSPRNG keyingi bit testini qanoatlantiradi va tizim holatining buzilishiga qarshi turadi. Talab qilinadigan xavfsizlik darajasiga qarab, CSPRNG dasturiy ta’minot komponentlari, apparat qurilmalari yoki ularning kombinatsiyasi sifatida amalga oshirilishi mumkin.

§1.4-paragrafda simmetrik blokli shifrlash algoritmlarida raund kalitlari tahlili va mavjud oqimli shifrlash algoritmlari tahlil qilingan. Simmetrik shifrlash algoritmlari uchun raund kalitlar generatsiyasi bo‘yicha tadqiqotlar yetarli emasligi aniqlandi. Shuningdek oqimli shifrlash algoritmlarini ilovaga maxsus integrallashgan sxema (ASIC) va maydonli dasturlanadigan mantiqiy massiv (FPGA) muhitida, dasturiy vosita ko‘rinishida amalga oshirilgan parametrlarning qiyosiy tahlil natijalari jadval shaklida taqdim etilgan. Oqimli shifrlash algoritmlarini apparat va dasturiy ko‘rinishda amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmlarini yaratish hamda ularni baholash bo‘yicha tadqiqotlar yetarli emasligi aniqlandi. Ularning xususiyatlari va bardoshliligi bo‘yicha ma’lumotlar 1-jadvalda keltirilgan.

1-jadval

Psevdotasodifiy sonlar generatorlarining kriptobardoshligi xususiyatlar tahlili

Algoritm nomi	Kalit uzunligi (bit)	Tarkibidagi amallar soni	Ishlash samaradorligi	Kriptobar-doshligi
Kongruent generatorlar	<64	Ko‘paytirish, mod N	Tezligi past	$<2^{64}$, bardoshsiz
Salsa20	128	O‘nga surish, XOR	Tezligi yuqori	2^{160}, yuqori
ANSI X9.17 FIPS-186 YARROW-160	64-160	3DES, 2DES, SHA-1 algoritmlari	Tezligi past, faqat kalit ishlab chiqish uchun	2^{128}, yuqori
ISAAK Algoritmi	64	Siljitish registri	Takrorlanmas davri kichik	2^{64}, kichik
A5	64	Siljitish registrlari kombinatsiyasi	Tezligi yuqori	2^{64}, kichik
RC-4,	2048 bitgacha	Mod256, o‘rin almashtirish	Tezligi yuqori, patentga yega	2^{64}, kichik
Spritz	2048 bitgacha	Mod256, o‘rin almashtirish	Tezligi yuqori	2^{128} yuqori

Salsa20 va ANSI X9.17, Spritz kabi algoritmlar yuqori kriptobardoshlikka ega. RC4 va ISAAC kabi algoritmlar tezligi yuqori bo‘lsada zaif hisoblanadi.

Dissertatsiyaning **«kriptografik bardoshli kalitlarni ishlab chiqish usullari»** deb nomlangan ikkinchi bobida simmetrik blokli shiflash algoritmlari uchun raund kalitlarini generatsiya qiladigan algoritm ishlab chiqilgan. Shuningdek, apparat ko‘rinishida amalga oshirishga qulay bo‘lgan AAOOSHA128 deb nomlangan oqimli shifrlash algoritmi va dasturiy ko‘rinishda amalga oshirishga qulay bo‘lgan massiv elementlarini uzluksiz almashtirishga asoslangan MEAG deb nomlangan oqimli shifrlash algoritmi ishlab chiqilgan, bundan tashqari, kriptografik psevdotasodifiy sonlar generatorining gibrid modeli yaratilgan.

§2.1-paragrafda simmetrik blokli shifrlash algoritmlari uchun kalit generatsiyalash algoritmi taklif etilgan.

Taklif etilgan raund kalitlarini generatsiyalash algoritmida dastlab shifrlash kaliti 256 bit va 256 bit insilizatsiya vektoridan foydalaniladi. K maxfiy kalit va intilizatsiya vektorining har biri 4 ta 64 bitli qismlarga bo‘linadi. Ushbu qismlarning belgilanishi quyida keltirilgan. Algoritm almashtirishlar va o‘zgarmaslardan foydalanidigan, xususan, Rotation – aralashtirish funksiyasi, S – chiziqsiz almashtirish funksiyasi(S blok), R – ikkita massiv elementlarini 2 modul bo‘yicha qo‘shish funksiyasi, C_0 dan C_4 gacha nomlangan o‘zgarmas konstanta qiymatlardan iborat. Dastlab S – chiziqsiz akslantish orqali 8 bitli massiv elementlarini quyidagi S blokdagi mos 8 bitli qiymatlar bilan almashtiradi.

$S = \{182, 99, 75, 57, 194, 175, 102, 209, 192, 180, 244, 230, 210, 116, 166, 89, 82, 108,$
$229, 190, 208, 37, 155, 203, 91, 9, 43, 45, 164, 103, 113, 32, 97, 133, 216, 202, 144,$
$170, 83, 141, 254, 248, 63, 76, 73, 131, 27, 225, 137, 231, 217, 136, 228, 107, 55, 48,$
$247, 29, 172, 134, 64, 179, 88, 7, 59, 149, 213, 105, 125, 165, 163, 140, 47, 85, 94, 39,$
$146, 70, 69, 173, 65, 38, 159, 100, 130, 56, 184, 26, 68, 98, 0, 30, 115, 96, 151, 167, 74,$
$10, 51, 78, 80, 40, 232, 220, 188, 176, 148, 122, 222, 236, 15, 224, 3, 185, 34, 124, 246,$

214, 121, 215, 201, 67, 168, 62, 169, 36, 245, 223, 87, 13, 189, 195, 128, 198, 84, 109,
126, 138, 53, 255, 61, 25, 117, 50, 177, 178, 158, 157, 111, 120, 145, 243, 199, 154, 123,
16, 41, 150, 161, 21, 135, 93, 183, 156, 71, 19, 114, 191, 18, 118, 12, 8, 86, 14, 112, 181,
204, 206, 58, 253, 162, 104, 42, 242, 171, 72, 200, 234, 81, 44, 52, 235, 31, 211, 212, 127,
152, 237, 11, 6, 160, 143, 106, 227, 174, 2, 132, 5, 79, 142, 1, 139, 66, 60, 28, 129, 33, 239,
92, 226, 90, 101, 24, 249, 193, 95, 205, 20, 187, 241, 54, 23, 186, 153, 46, 147, 219, 240,
119, 233, 77, 4, 197, 35, 218, 250, 196, 251, 22, 49, 110, 207, 17, 252, 221, 238}

Shundan so‘ng, Rotation ya’ni almashtirish funksiyasi, 64 bitli massiv elementlarini quyidagicha almashtiradi: a_0, a_1, ..., a_7 massiv qiymatlarini mos ravishda a_0 massiv surilmaydi, a_1 massiv 1 bitga, a_2 massiv esa 2 bitga va hakozo a_7 massiv 7 bitga siklik suriladi. Shundan so‘ng, a_7 massiv boshiga qolgan massivlar bir bayt o‘nga suriladi.

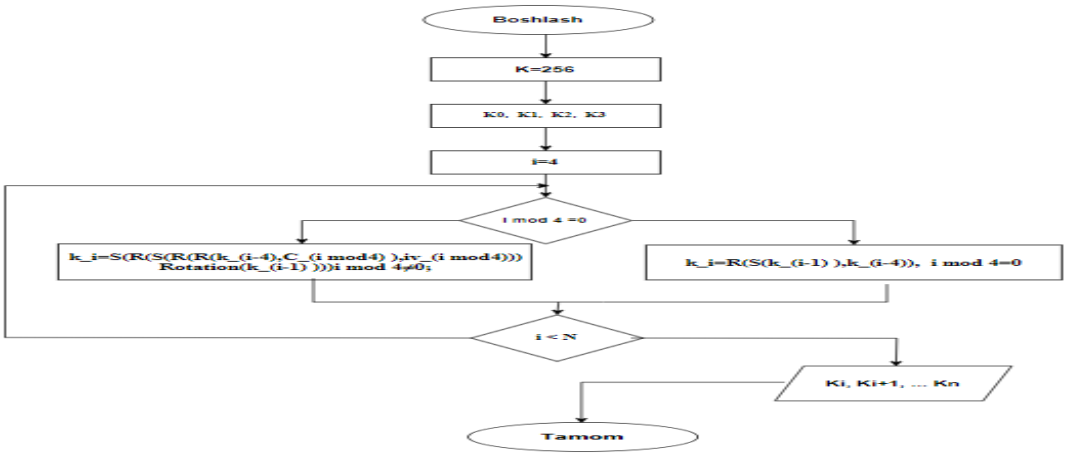
$$a_0 = a_0$$
$$a_1 = a_1 \lll 1$$
$$a_2 = a_2 \lll 2$$
$$a_3 = a_3 \lll 3$$
$$a_4 = a_4 \lll 4$$
$$a_5 = a_5 \lll 5$$
$$a_6 = a_6 \lll 6$$
$$a_7 = a_7 \lll 7$$
$$\{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \rightarrow \{a_7, a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$$

Natijada n ta raund uchun shifrlash kalitlarini generatsiya qilish uchun $N = 4 * (n + 1)$ $(i = 1,2, \dots, n)$ ta qadamdan iborat quyidagi formulalar orqali hisoblandi.

$$k_i = S\left(R\left(S\left(R(R(k_{i-4}, C_{i \bmod 4}), iv_{i \bmod 4})\right), Rotation(k_{i-1})\right)\right), i \bmod 4 \neq 0; \quad (2.1)$$

$$k_i = R(S(k_{i-1}), k_{i-4}), \ i \bmod 4 = 0; \quad (2.2)$$

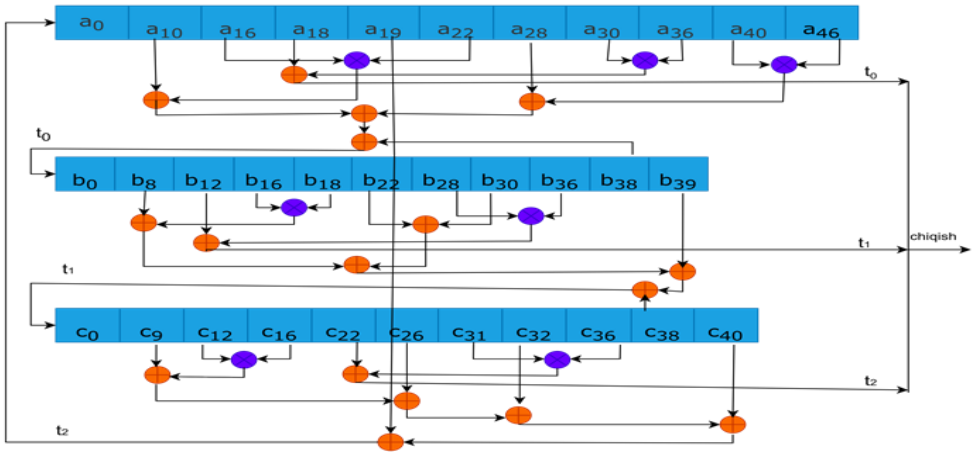
$i = 0,1, \dots, n$ raundlarning kalitlarini shakllantirishda hosil qilingan k_i massivlar qiymatlaridan istalgan va takrorlanmas ketma-ketlikda foydalanishi mumkin. Raund kalitlarini generatsiya qiladigan algoritm blok-sxemasi 2-rasmda keltirilgan.



2-rasm. Raund kalitlarini generatsiya qiladigan algoritm blok-sxemasi

1-tasdiq. Chiziqsiz almashtirish va siklik siljitish operatsiyalariga asoslangan simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini generatsiya qilish algoritmi yuqori tasodifiylikni ta'minlaydi.

§2.2-paragrafda AAOOSHA128 (Apparatda amalga oshiriladigan oqimli shifrlash algoritm) ning boshlang‘ich holati umumiy uzunligi 128 bit bo‘lgan 47, 40 va 41 bit bo‘lgan 3 ta siljitish registridan tuzilgan. Har bir holat o‘ngga siklik siljitish registrlaridagi bitlarni chiziqsiz uzatish va qayta aloqa kombinatsiyasi orqali o‘zgartiriladi. Shifrni ishga tushirish uchun 128 bit uzunlikga ega K maxfiy kalit 3 siljitish registrlariga berilgan qoida bo‘yicha yoziladi va initsializatsiya jarayoni 40*41 = 1640 iteratsiyada bajariladi, bu esa boshlang‘ich holatning har bir biti kalitning har bir bitiga bog‘liqligini kafolatlaydi. Unda 7 ta AND va 18 ta XOR elementlaridan foydalaniladi. AAOOSHA128 algoritmning funksional sxemasi 3-rasmda keltirilgan.



3-rasm. AAOOSHA128 algoritmning funksional sxemasi.

Algoritm 128 bitli kalitni 128 bitli Initsializatsiya vektori bilan 2 modul bo‘yicha qo‘shib, 128 (47+40+41) bitli boshlang‘ich holat registrlari quydagi psevdokod orqali bajariladi.

$K = K \oplus IV$
$(K_0, K_1, \dots, K_{46}) \rightarrow (a_0, a_1, a_2, \dots, a_{46})$
$(K_{47}, K_{48}, \dots, K_{86}) \rightarrow (b_0, b_1, b_2, \dots, b_{39})$
$(K_{87}, K_{88}, \dots, K_{127}) \rightarrow (c_0, c_1, \dots, a_{40})$
$for\ i = 0\ to\ 1640\ do$
$a_{10} \oplus a_{16} \cdot a_{22} \oplus a_{28} \oplus a_{40} \cdot a_{46} \oplus b_{38} \rightarrow t_0$
$b_8 \oplus b_{16} \cdot b_{18} \oplus b_{22} \oplus b_{30} \oplus b_{39} \oplus c_{38} \rightarrow t_1$
$c_9 \oplus c_{12} \cdot c_{16} \oplus c_{26} \oplus c_{32} \oplus c_{40} \oplus a_{19} \rightarrow t_2$
$(t_2, a_0, \dots, a_{45}) \rightarrow (a_0, \dots, a_{46})$
$(t_1, b_0, \dots, a_{38}) \rightarrow (b_0, \dots, b_{39})$
$(t_0, c_0, \dots, c_{39}) \rightarrow (c_0, \dots, c_{40})$
$end\ for.$

AAOOSHA128 ichki holati teskari tarzda yangilanadi va ($c_0, .., c_{40}$) registrining ishga tushirilishi holatning 40 iteratsiyadan kamroq aylanishining oldini oladi. AAOOSHA128da psevdotasodifiy ketma-ketliklarni hosil qilish uchun teskari aloqa tenglamasidan foydalanadi:

$$s(t+1) = (a_1 s(t) \oplus a_2 s(t-1) \oplus \dots \oplus a_n s(t-n+1)) \bmod 2 \qquad (2.3)$$

bu yerda: $s(t)$ - t vaqtdagi holati, a_i- teskari aloqa koeffitsiyentlari ($a_i \in \{0,1\}$).

Teskari aloqa funksiyasi sifatida primitiv ko‘phadlardan foydalanish odatiy holdir. Xarakteristik f(x) ko‘phadning xossasini "k-tartibli primitiv ko‘phad" bilan baholash mumkin, u quyidagicha aniqlanadi: berilgan, $f(x) = \sum_{i=0}^{n} a_i x^i, n > k,$

$a_i \in GF(2), i = 0,1,\dots,n, f(x)$ -tartibli primitiv ko‘phad deyiladi, agar $f(x) = (x+1)^k \cdot g(x)$ bo‘lsa, bu yerda - $g(x)$ ham primitiv ko‘phad bo‘ladi. $f(x)$ da ko‘rsatilgan indekslardagi bitlar 2 modul bo‘yicha qo‘shilib yangi bit hosil qilinishi quydagicha amalga oshiriladi:

$$s_{n+1} = s_{n-132} \oplus s_{n-129} \oplus s_{n-123} \oplus \cdots \oplus s_{n-3} \oplus s_n \qquad (2.4)$$

Natijada f(x) ko‘phaddagi har bir darajaga mos **bit indekslari**ni quyidagicha yozish mumkin:

$$f(x) = x^{132} + x^{129} + x^{126} + x^{120} + x^{114} + x^{108} + x^{87} + x^{75} + x^{72} + x^{63} + x^{60} + x^{57} + x^{54} + x^{48} + x^{45} + x^{33} + x^{27} + x^{21} + x^{12} + x^9 + x^6 + 1$$

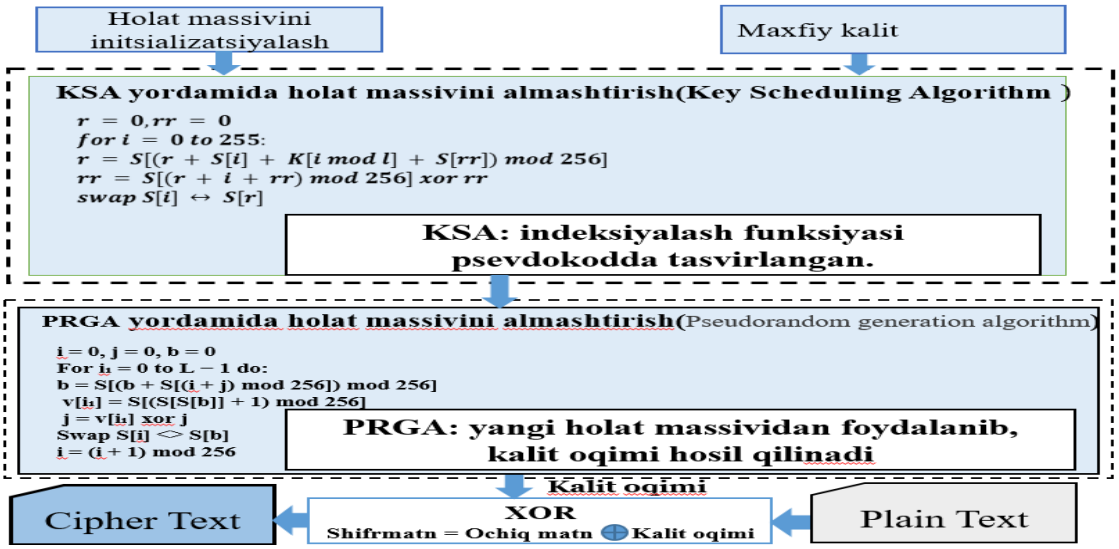
2-teorema: Agar AOOSHA128 algoritmning xarakteristik ko‘phadi $f(x) = (x^3+1)^3 \cdot g(x^3)$ ko‘rinishga ega bo’lsa, u holda $f(x)$ko’phad uchinchi tartibli primitiv ko‘phad bo’ladi.

Hisoblash natijasida kriptografik PRNG yoki oqimli shifrlovchi bit hosil bo‘ladi.

2-tasdiq. AAOOSHA128 oqimli shifrlash algoritmi apparatda amalga oshirish uchun optimallashtirilgan bo‘lib, chiziqsiz teskari aloqali siljitish registrlari va primitiv ko‘phadlar asosida yuqori xavfsizlik va samaradorlikni ta'minlaydi.

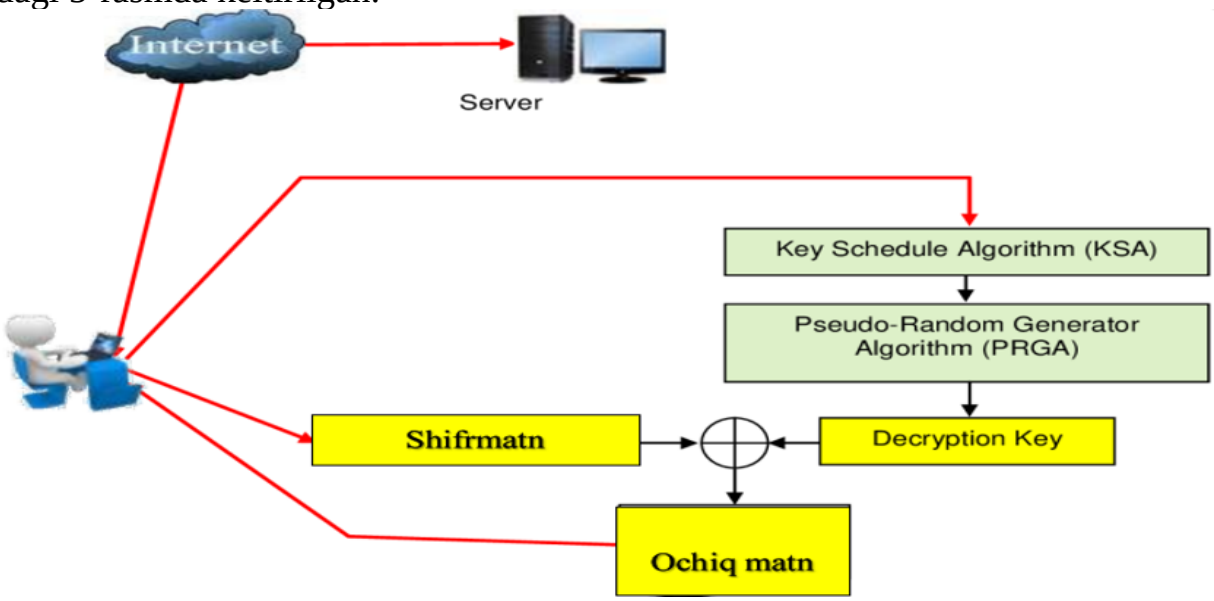
Natijada generatsiya qilingan kalitlarning ishonchliligini maksimal ta’minlanishini kafolatlash maqsadida 128 bit maxfiy kalit yordamida 2^{64} bit uzunlikgacha bo‘lgan kalit generatsiya qilish mumkin.

§2.3-paragrafda dasturiy ko‘rinishda amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmi — MEAG (massiv elementlarini almashtiradigan generator) ishlab chiqilgan bo‘lib, u kalitlarni yaratish jarayonida RC4 algoritmiga o‘xshash, ammo yordamchi o‘zgaruvchilar tomonidan kiritilgan qo‘shimcha murakkablik bilan massiv elementlarini uzluksiz almashtirishga asoslanadi. Oqimli shifr sifatida algoritmining asosiy protsedurasi uchta jarayondan iborat: Kalitlarni rejalashtirish algoritmi (KSA), psevdotasodifiy generatsiyalash algoritmi (PRGA) va shifrlash yoki deshifrlash jarayonidan iborat. MEAG genetatorining ishlash sxemasi 4-rasmda keltirilgan.



4-rasm. MEAG genetatorining ishlash sxemasi

Kalitni rejalashtirish (KSA) jarayoni — bu 256 elementli *S* massivni initsializatsiya qilish va uni kalitga bog‘liq bo‘lgan aralashma (PRGA) ga aylantirishdan iborat. Unda S massiv 256 ta o‘rin almashtirish (swap) jarayoni bajariladi va bu jarayon r, rr va i indekslari orqali boshqariladi. PRGA bosqichida esa shifrlash jarayoni baytlarni ketma-ket generatsiyalab kalit oqimini hosil qiladi. Har bir iteratsiyada i, j, b kabi indekslar algoritm ichida yangilanadi va S massivida dinamik o‘rin almashish sodir bo‘ladi. Natijada PRGA bosqichi shifrlash jarayonida baytlarni ketma-ket generatsiyalab kalit oqimini hosil qiladi. Massiv elementlarini almashtiruvchi generator yordamida shifrlangan ma’lumotlarni deshifrlash kaliti bilan shifrlangan matnni 2 modul bo‘yicha qo‘shish amali yordamida ochadi. Shuningdek, MEAG algoritmining sxemasi quyidagi 5-rasmda keltirilgan.



5-rasm. MEAG algoritmining sxemasi

Kalitlarni tasodifiy generatsiyalash jarayonida MEAG ishlash algoritmi juda ishonchli hisoblanib shifrlash va deshifrlash uchun qisqa vaqt talab qiladi. MEAG algoritmida shifrlash va deshifrlash jarayonida RC4 da aniqlangan Brute-force va Flarere-Mantin-Shamir hujumlariga nisbatan bardoshli hisoblandi.

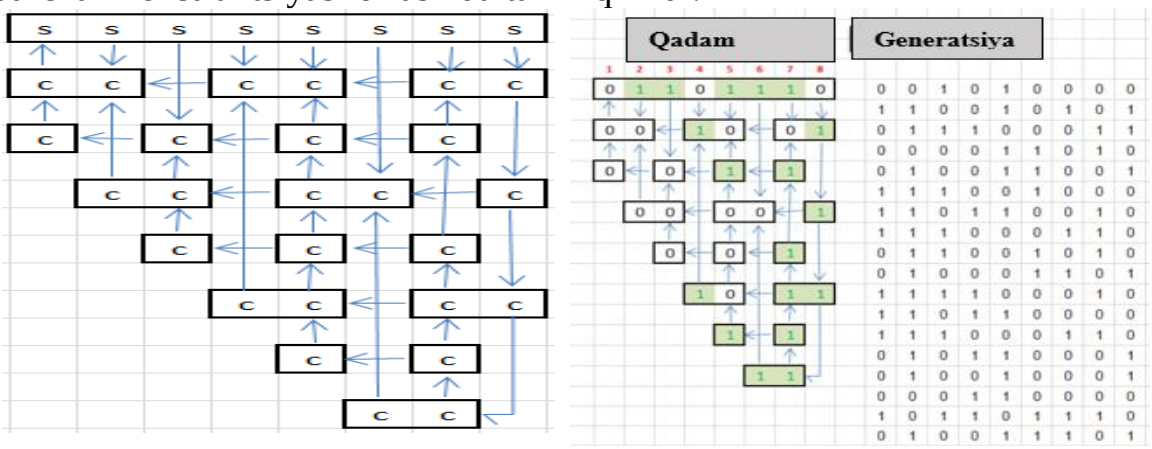
3-tasdiq. MEAG algoritmi massiv elementlarini dinamik almashtirish va chiziqsiz akslantirishlarga asoslangan bo‘lib, RC4 algoritmiga nisbatan yuqori xavfsizlikni ta'minlaydi.

§2.4-paragrafda teskari aloqali siljitish registrlari usuliga asoslangan PRNG generatorlaridan biri, “Weyl o‘rtacha kvadrati” ketma-ketligi tezkor ishlashi bilan alohida qiziqish uyg‘otadi. Weyl psevdotasodifiy generatori - bu tasodifiy sonlar ketma-ketligini hosil qilish uchun kvadrat va modul operatsiyalaridan foydalanadigan algoritm.

$$w_{i+1} = w_i + s,$$
$$x_{i+1} = {x_i}^2 + w_{i+1},$$
$$y_{i+1} = (x_{i+1} \bmod 2^{64}) \gg 32, \qquad (2.5)$$

Weyl algoritmining zaif tomonlarini himoya qilish uchun quyidagi sxema bo‘yicha PRNG ning gibrid versiyasidan foydalanish taklif etiladi. Ikki qismdan

iborat kalit kiritiladi, unda teskari aloqali siljitish registrini quyidagi turdagi uchburchak konstruktsiyasi 6-rasmda taklif qilindi.

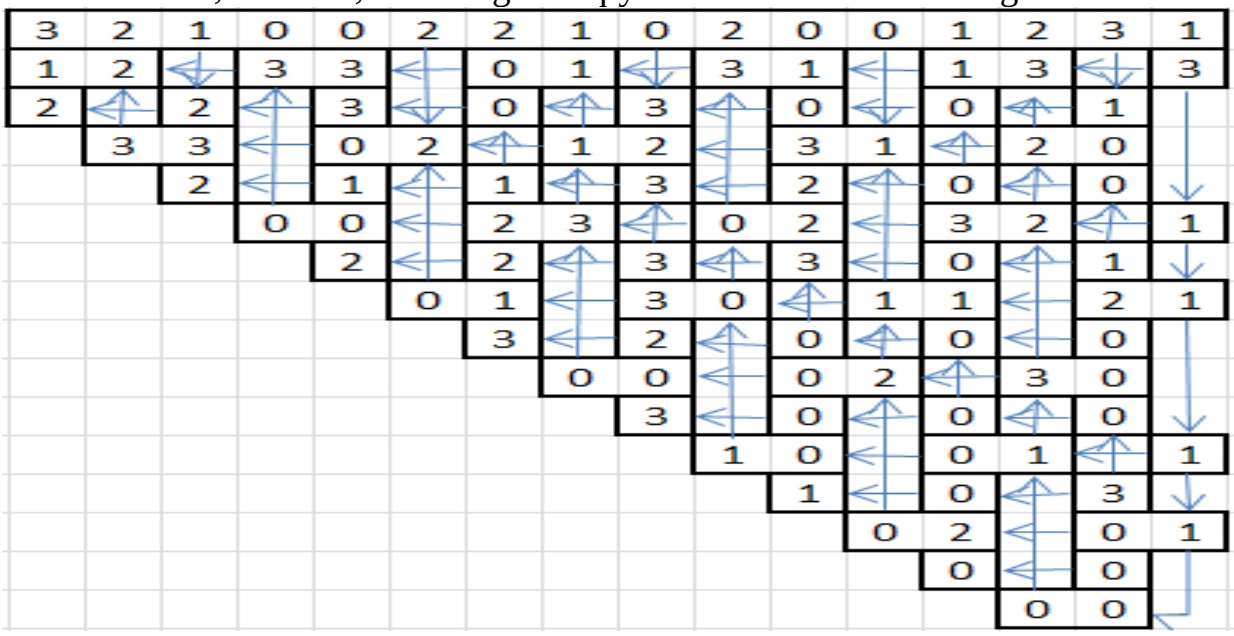


6-rasm. Teskari aloqali siljitish registrini uchburchak konstruktsiyasi

S tuzilma modeli PRNG ning asosiy xotira strukturasini yaratadi, c tuzilma esa s xotiraga bog‘liq holda psevdo tasodifiy sonlar generatorining ishlashini tavsiflaydi. U tasodifiy sonlar ketma-ketligining uzunligi nafaqat raqamlar soniga, balki c ichki registrlar holatlariga ham bog‘liq bo‘ladi.

$$M \approx 2^{0,35*n^2+n}, \qquad (2.6)$$

n - raqamlar soni. M- tasodifiylik sikl uzunligi. Sikl uzunligi qancha kichik bo‘lsa PRNG tezda takrorlanadi. Teskari aloqali registrini dasturiy ta'minotni amalga oshirishning o‘ziga xos xususiyati shundaki, hujayralar nafaqat bit qiymatlarini, balki " *n /2* " dan oshmaydigan boshqa qiymatlarni ham o‘z ichiga olishi mumkin, masalan, 0 dan 3 gacha qiymatlari 7-rasmda keltirilgan.

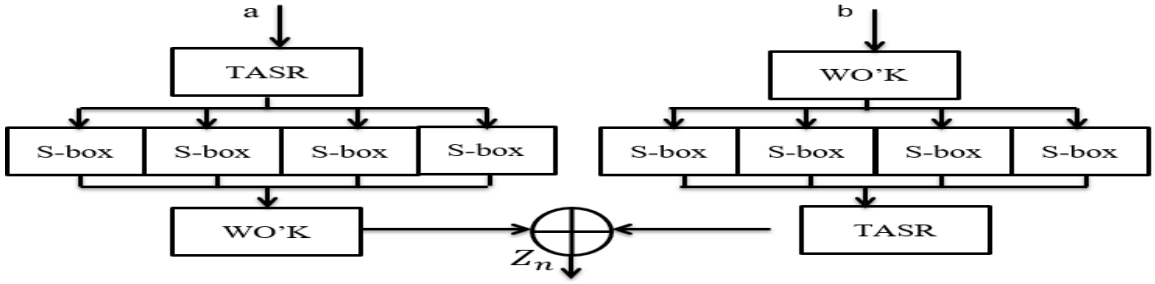


7-rasm. 0 dan 4^{16} gacha bo‘lgan raqamlarning teskari aloqali registori

Gibrid modelning davriyligini oshirish maqsadida M ning qiymatini quydagicha o‘zgartirish mumkin.

$$M \approx c^{0,35*n^2+n} \qquad (2.7)$$

Taklif etilayotgan Gibrid modelning umumiy ko‘rinishi quydagi 8-rasmda keltirilgan.



8-rasm. Gibrid PRNG ning umumiy sxemasi.

TASR(Teskari aloqa siljitish registrlari) va WO‘K(*Weyl o‘rtacha kvadrati)* oqimi hosil qilgan psevdotasodifiy sonlardan kelib chiqadigan ketma-ketliklar S-box o‘tkazilganda teskarisiga almashadi. Shundan so‘ng 2 modul qo‘shish amali bilan hisoblanadi. Natija gibrid PRNG ning quyidagi matematik ifodaga ko‘rinishiga keladi:

$$Z_n = Y_n\left(S(\sum_{i=0}^{L-1} c_i \cdot X_{n-i} \bmod 2)\right) \oplus X_n\left(S\left((Y_n + w)\bmod c^{0,35*n^2+n}\right)\right) \qquad (2.8)$$

Ushbu model bilan tasodifiy sonlarni yaratish sxemasiga chiziqli bo‘lmagan funksiya qo‘shiladi, shifrlashning ikkala turi bir-birini to‘ldiradi va chiqish gammasi tizimning ichki holatini tahlil qilishga to‘sqinlik qiladi.

4-tasdiq. Teskari aloqali siljitish registrlari va Weyl o‘rtacha kvadrati ketma-ketligiga asoslangan gibrid PRNG modeli chiziqsiz funksiyalar orqali yuqori tasodifiylik va kriptografik xavfsizlikni ta'minlaydi.

Dissertatsiya ishining «**Ishlab chiqilgan kriptografik bardoshli kalitlarni kriptotahlil usullari yordamida baholash va taqqoslash**» nomlangan uchinchi bobida simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini generatsiya qilish algoritmi, shuningdek, apparat hamda dasturiy amalga oshirishga qulay bo‘lgan oqimli shifrlash algoritmlarining kriptotahlil usullariga baholash natijalari keltirilgan. §3.1-paragrafda taklif qilingan algoritmlarni tasodifiylik testlariga baholash baholash natijalari keltirilgan. Xususan, raund kalitlarini generatsiya qiladigan algoritmni 2-jadvalda NIST(National Institute of Standards and Technology) statistik testalari orqali testdan o‘tkazildi.

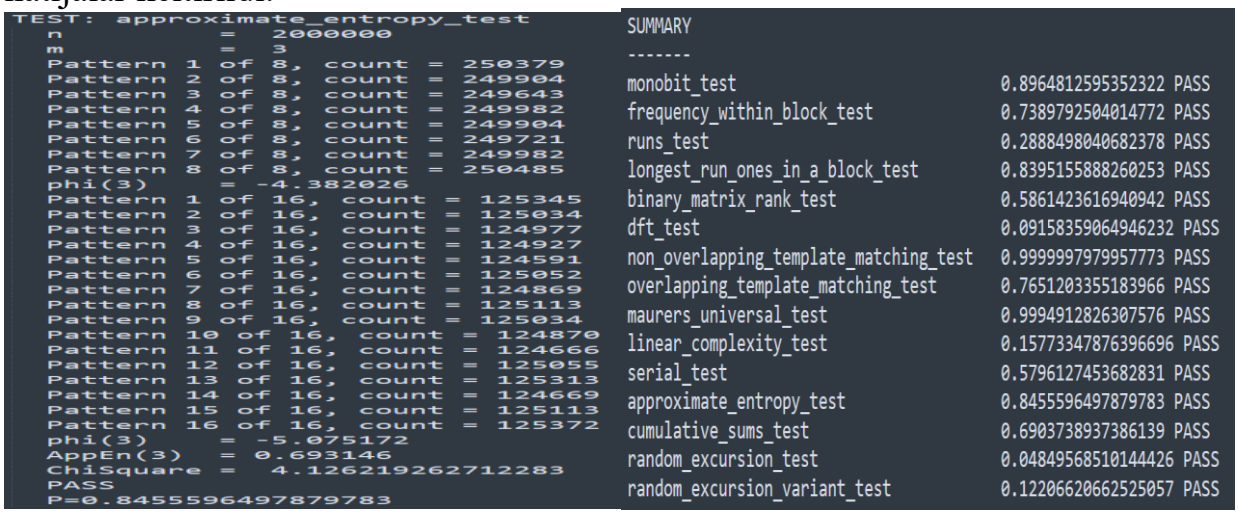
2-jadval

Raund kalitlarini generatsiyasini NIST statistik testida baholash

Test nomi	Natija (p-value)	Holat	Muvaffaqiyatli diapazon
monobit_test	0.8975605639	PASS	0.01-0.99
frequency_within_block_test	0.2708842358	PASS	0.01-0.99
runs_test	0.5036686676	PASS	0.01-0.99
longest_run_ones_in_a_block_test	0.9553989385	PASS	0.01-0.99
binary_matrix_rank_test	0.2201007292	PASS	0.01-0.99
dft_test	0.3752687226	PASS	0.01-0.99
non_overlapping_template_matc hing_test	0.9999648101	PASS	0.01-0.99
overlapping_template_matching_ test	0.5733547337	PASS	0.01-0.99
maurers_universal_test	0.0987345585	PASS	0.01-0.99
linear_complexity_test	0.7387164598	PASS	0.01-0.99
serial_test	0.8419852083	PASS	0.01-0.99
approximate_entropy_test	0.8818725039	PASS	0.01-0.99
cumulative_sums_test	0.6144715890	PASS	0.01-0.99
random_excursion_test	0.2025454198	PASS	0.01-0.99
random_excursion_variant_test	0.0194967674	PASS	0.01-0.99

NISTda har bir bosqichda testni hisoblash orqali *p* – qiymat topiladi. Olingan natijalar orqali ketma-ketlikni testlashdan o‘tgan/o‘tmaganligi aniqlanadi. Agar p-qiymat [0,1] oraliqda bo‘lsa testlashdan o‘tgan bo‘ladi.

AAOOSHA128 algoritmida ham yuqorida berilgan kalit yordamida generatsiya qilingan ketma-ketliklar NIST statistik testlari yordamida tasodifiylik darajasi baholandi. Baholash natijalari yaxshi natija ko‘rsatdi. Quyida mazkur test tarkibidagi taxminiy entropiya testi va umumiy 15 ta test bo‘yicha olingan natijalar keltirildi.



9-rasm. AAOOSHA128 algoritmini NIST statistik testi orqali baholash natijalari

Taklif etilgan MEAG algoritmining NIST testidan foydalanib shifrlangan 1000000 bit bo‘yicha tasodifiy natijalari 3-jadvalda keltirilgan.

3-jadval.

MEAG algoritmini Nist testida baholash

Test nomi	Natijalar qiymati	Holati	Muvaffaqiyatli diapazon
monobit_test	0.881368	Pass	0.01-0.99
frequency_within_block_test	0.781296	Pass	0.01-0.99
runs_test	0.596638	Pass	0.01-0.99
longest_run_ones_in_a_block_tes t	0.752839	Pass	0.01-0.99
binary_matrix_rank_test	0.860583	Pass	0.01-0.99
dft_test	0.639160	Pass	0.01-0.99
non_overlapping_template_matc hing_test	0.691478	Pass	0.01-0.99
overlapping_template_matching _test	0.224202	Pass	0.01-0.99
maurers_universal_test	0.805704	Pass	0.01-0.99
linear_complexity_test	0.117861	Pass	0.01-0.99
serial_test	0.597103	Pass	0.01-0.99
approximate_entropy_test	0.809020	Pass	0.01-0.99
cumulative_sums_test	0.876226	Pass	0.01-0.99
random_excursion_test	0.914524	Pass	0.01-0.99
random_excursion_variant_test	0.985330	Pass	0.01-0.99

NIST statistik testlaridan olingan xulosalar generatorlarning ishonchliligini baholaydi. Yuqorida keltirilgan kalit generatsiya qilish algoritmlari matematik asoslarda qurilgan bo‘lib, tasodifiylikning yuqori darajasini ta'minlaydi va NIST testlaridan muvaffaqiyatli o‘tishi ularning xavfsizligini isbotlaydi.

§3.2-paragrafda taklif qilingan algoritmlarni kriptobardoshligini kriptotahlil usullari yordamida baholash natijalari keltirilgan. Birinchi simmetrik blokli shifrlash algoritmlarida raund kalitlarida qo‘llaniladigan bir bitli siklik siljitish amali uchun chiziqli algebraik tenglamalar keltirib chiqarilgan.

$$y_0 = x_7 \oplus x_6x_5x_4 \oplus x_3x_2x_1 \oplus x_0$$
$$y_1 = x_7x_6x_5 \oplus x_4x_3x_2 \oplus x_1x_0$$
$$y_2 = x_7x_6x_5x_4x_3 \oplus x_2x_1x_0 \oplus x_7$$
$$y_3 = x_7x_6x_5 \oplus x_4x_3x_2x_1 \oplus x_0x_7x_6$$
$$y_4 = x_7x_6x_5x_4 \oplus x_3x_2x_1x_0 \oplus x_6x_4x_2$$
$$y_5 = x_7x_6x_5x_4x_3 \oplus x_2x_1x_0x_7x_6 \oplus x_4x_3$$
$$y_6 = x_7x_6x_5x_4x_3x_2 \oplus x_1x_0x_7x_5 \oplus x_4x_2x_1$$
$$y_7 = x_7x_6x_5x_4x_3x_2x_1 \oplus x_0x_7x_6x_5 \oplus x_4x_3x_2$$

Har bir almashtirish uchun algebraik tenglamalar shakllantirilgandan so‘ng, ularni birlashtirish orqali bir raund uchun tenglamalar shakllantiriladi. Natijada raund kalitlarni generatsiyalash uchun algebraik kriptotahlil usuli yordamida tuzilgan tenglamalarning parametrlari 4-jadvalda keltirilgan.

4-jadval

Algoritm uchun algebraik kriptotahlil usuli yordamida shakllantirilgan tenglamalar parametrlari

Iteratsiya	Noma’lumlar soni o’zgarishi	Murakkablik soni O(n^3)
2	2^{14}	2^{42}
3	2^{16}	2^{48}
4	2^{20}	2^{60}
5	2^{22}	2^{66}
6	2^{42}	2^{126}
7	2^{44}	2^{132}
8	2^{48}	2^{144}
9	2^{50}	2^{150}
10	2^{88}	2^{264}

Ushbu jadvalda algebraik kriptotahlili initsializatsiya jarayonining 7 iteratsiyasidan boshlab yechish murakkabligi tufayli algebraik kriptotahlilga bardoshli deb xulosa qilish mumkin. Taklif qilingan algoritmni kriptobardoshligini chiziqli va differensial kriptotahlil usullari yordamida ham baholash natijalari quyidagi 5-jadvalda keltirilgan.

5-jadval.

Kriptotahlil usullari yordamida baholash

Algoritm	Raund kalitlarini generatsiya qilish algoritmi
Algebraik kriptotahlil	Initsializatsiya siklining 7-iteratsiyasida 2^{132} murakkablik hosil qiladi
Differensial kriptotahlil	Initsializatsiya siklining 6- iteratsiyasidan keyin differensial ehtimollik 2^{-414} daraja tushadi. Differensial kriptotahlilga bardoshli bo’ladi.
Chiziqli kripotahlil	7-iteratsiyada chiziqli tahlilni 2^{-8} bo’lganda aniqlash imkoni bo’lmaydi

AAOOSHA128 algoritmiga algebraik kriptotahlil usuli yordamida shakllantirilgan tenglamalarning parametrlari quyidagi 6-jadvalda keltirilgan.

6-jadval

AAOOSHA128 algoritmini algebraik kriptotahlil usuli yordamida baholash

Tenglamalar sistemasining minimal darajasi	**Iteratsiya qadami**	**Noma'lumlar soni**	**Murakkablik $O(n^3)$**
2-daraja	47	2^7	2^{21}
3-daraja	47+40=87	2^{14}	2^{21}
4-daraja	87+41=128	2^{21}	2^{63}
5-daraja	128+47=175	2^{28}	2^{84}
6-daraja	175+40=215	2^{35}	2^{105}
7-daraja	215+41=256	2^{42}	2^{126}
8-daraja	256+47=303	2^{49}	2^{147}

AOOSHA128 shifrlash algoritmining initsializatsiya jarayonida, 303-iteratsiyadan so‘ng noma’lum o‘zgaruvchilar sonining keskin oshib ketishi (2^{49}) va ushbu tenglamalar tizimini yechishning yuqori murakkabligi (2^{147}) sababli, mazkur algoritm algebraik kriptotahlil usullariga nisbatan bardoshli ekanligini xulosa qilish mumkin. Yuqoridagi natijalardan kelib chiqib Trivium va AAOOSHA128 algoritmlarining kriptotahlil usullariga baholash natijalari 7-jadvalda keltirilgan.

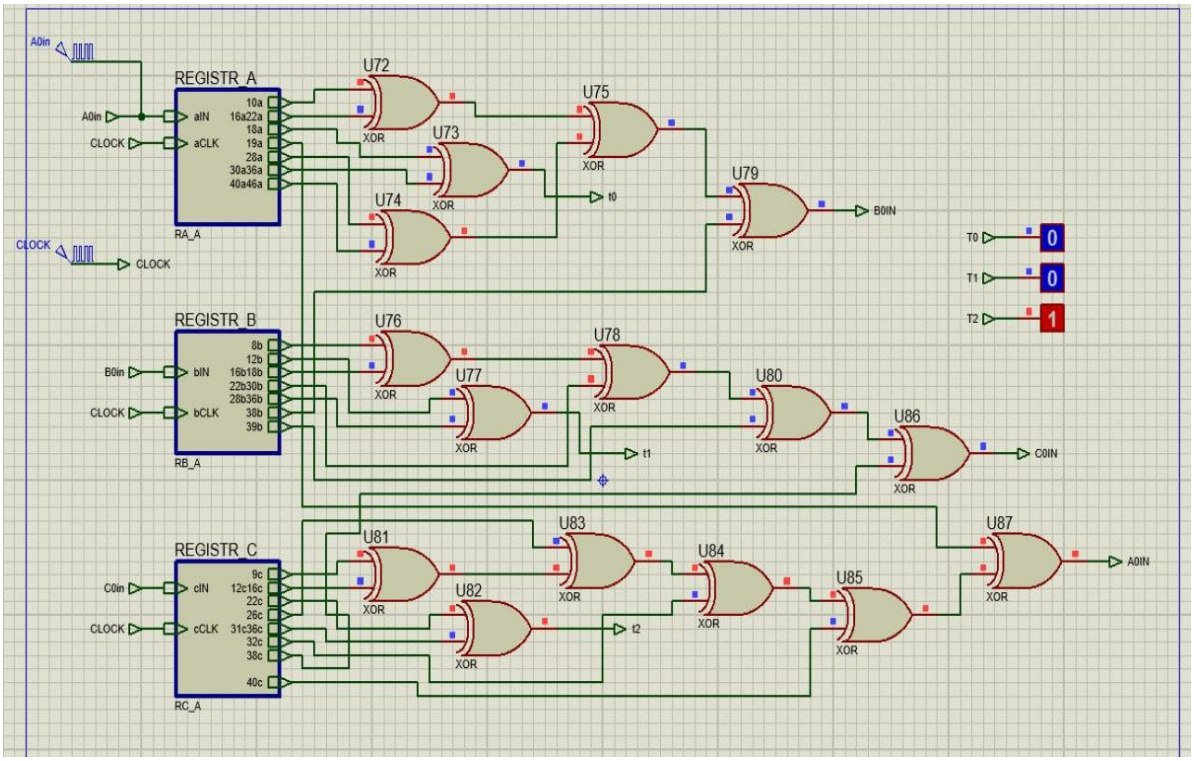
7-jadval.

AAOOSHA128 algoritmini kriptotahlil usullari yordamida baholash

Algoritm	**Trivium**	**AOOSHA128 (mazkur ish)**
Algebraik kriptotahlil	Initsializatsiya siklining 325-iteratsiyasida $2^{42.2}$ noma’lum	Initsializatsiya siklining -256 iteratsiyasida 2^{42} noma’lum
Differensial kriptotahlil	Initsializatsiya siklining 961-iteratsiyasidan keyin bardoshli	Initsializatsiya siklining 412-iteratsiyasidan keyin bardoshli
Chiziqli kriptotahlil	Initsializatsiya siklining 564-iteratsiyasida 2^{129} noma’lum	Initsializatsiya siklining 337-iteratsiyasida 2^{129} noma’lum

§3.3-paragrafda «ishlab chiqilgan algoritmlarni ma'lum generatorlar bilan parametrlar bo‘yicha taqqoslash va amalda qo‘llash natijalari» deb nomlangan bo’lib unda ishlab chiqilgan algoritmlar tezlik va amalga oshirish xususiyatlari bo’yicha baholangan. AAOOSHA128 psevdotasodifiy sonlar generatorining apparatda amalga oshirilish tartibi va ulardan olingan natijalar taqdim etilgan.

Proteus dasturida AAOOSHA128 algoritmini apparat ko‘rinishda amalga oshirish sxemasi 10-rasmda keltirib o’tilgan.



10-rasm. AAOOSHA128 algoritmini apparatda amalga oshirishning umumiy sxemasi

eStream tanlovida qatnashgan, apparat amalga oshirish qulay bo‘lgan oqimli shifrlash algoritmlari va AAOOSHA128 algoritmining apparatda amalga oshirish parametrlari 3.7-jadvalda keltirilgan.

8-jadval.

AAOOSHA128 algoritmi va eStream tanlovi ishtirokchi algoritmlarining tasodifiylik va tezkorlik bo‘yicha tahlili.

№	Algoritm nomi	Nist Spekial testlar to‘plamlari asosida tahlil natijasi (15 testdan)	Tezligi (Mbit/sek)
1.	**SalSa20**	15	450
2.	**ChaCha**	15	470
3.	**HC128**	12	378
4.	**HC256**	15	490
5.	**ISAAC**	15	415
6.	**AES CTR 128**	15	478
7.	**NSA**	15	330
8.	**AAOOSHA128**	15	342

Tahlil natijasiga ko‘ra taklif etilgan AAOOSHA128 algoritmining NIST statistik testidagi natijasi 15 taga teng bo‘lgan. AAOOSHA128 shifrlash usuli 342 Mbit/sek tezlikni tashkil qilgan.

MEAG algoritmining dasturiy ko‘rinishda amalga oshirish natijalarining dasturlash muhitida algoritmlarning omillar bo‘yicha tahlili (9-jadvalda qaysi holda yaxshi ko‘rsatkich bo‘lishi ham keltirilgan).

9-jadval.

Dasturlash muhitida algoritmlarning omillar bo‘yicha tahlili

Shir	Kalit uzunligi (bit)	IV (bit)	Ishga tushirish (sikl)	Shifrlash (sikl)	RAM (Kbayt)	ROM (Kbayt)	O‘tkazish qobiliyati (MBps)	CM
Yaxshisi			Pasti	Pasti	Pasti	Pasti	Yuqori	Pasti
Enocoro	128	64	512	1024	1.2	3.8	5.1	226
Salsa20	256	64	460	1024	2	5	9.7	278
HC-128	128	128	770	1536	2.5	4	7.9	262
AES-CTR	128	-	1024	2048	3	5	4.95	355
Spritz	128	-	256	1024	1.5	2.5	10.1	350
RC4	256	-	1024	2048	2	3	8.6	210
MEAG	256	-	512	1536	1.8	2.8	10.3	203

Dasturiy vositalar ko‘rinishda amalga oshirishda qulay bo’lgan oqimli shifrlash MEAG algoritmi tezkorlik va ishga tushirish vaqtining qisqaligi bilan qolganlaridan ajralib turadi. Xususan, MEAG algoritmi bilan IOT aparatlarida xavsizlik, tezkorlik va kam resurs talab qilishi asosida undan foydalanish mumkin.

XULOSA

Dissertatsiya ishida qo‘yilgan maqsad va vazifalarga muvofiq quyidagi natijalar olindi:

1. Simmetrik blokli shifrlash algoritmlari uchun raund kalitlarini generatsiya qilish algoritmi ishlab chiqildi. Ishlab chiqilgan algoritm o‘zgarishlar kiritilganda ham mustahkam raund kalitlarni ishlab chiqarish imkonini bergan.

2. Apparat ko‘rinishda amalga oshirishga mo’ljallangan oqimli shifrlash algoritmi ishlab chiqildi. Ishlab chiqilgan algoritm umumiy uzunligi 128 bit bo‘lgan 3 ta siljitish registrlaridan iborat, u apparat tarzda amalga oshirilganda Trevium algoritmiga nisbatan kam GATElar sonini talab qildi.

3. Massiv elementlarini almashtirishga asoslangan oqimli shifrlash algoritmi ishlab chiqildi. Ishlab chiqilgan dasturiy vosita shifrlash va rasshifrovkalash vaqti bo‘yicha 13 % samaradorlikka erishishga imkon bergan.

4. Tahlillar natijasida raund kalitlarini generatsiya qilish algoritmini algebraik kriptotahlil usuliga 7-iteratsiyasidan boshlab, chiziqliga 6-iteratsiyasidan keyin hamda differensialga 7-iteratsiyasidan keyin bardoshligini ko‘rsatdi. AAAOOSHA128 oqimli shifrlash algoritmi algebraik, chiziqli va differensial kriptotahlil usullariga nisbatan bardoshliligi tahlillar natijasida aniqlandi. Massiv elemementlarini almashtirishga asoslangan kalit generatsiyalash algoritmi ham kriptotahlil usullariga nisbatan bardoshliligi aniqlandi.

5. Ishlab chiqilgan oqimli shifrlash algoritmlari tezlik va amalga oshirish xususiyatlari bo‘yicha tahlil qilindi. Tahlil natijalariga ko‘ra taklif etilgan AAAOOSHA128 oqimli shifrlash algoritmining NIST statistik testlar to‘plamidagi natijsi 15 taga, tezligi esa 342 Mbit/sekni tashkil etdi.

6. MEAG algoritmi kalitga asoslangan soddalashtirilgan dasturiy algoritm bo‘lib, undan Internet buyumlar qurilmalarida (IOT) foydalanish mumkin. U xavfsizlik, tezlik va kamroq resurs talab qiladigan qurilmalarda foydalanish mumkin bo‘ladi.

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА
ПРИСУЖДАЮЩИЙ УЧЕНЫЕ СТЕПЕНИ
НАУЧНЫЙ СОВЕТ DSc.03/30.12.2019.FM.01.02

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

БОЗОРОВ АСКАР ХАИТМУРОТОВИЧ

РАЗРАБОТКА СТОЙКИХ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

05.01.05 – Методы и системы защиты информации.
Информационная безопасность.

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

Ташкент-2025

Тема диссертации доктора философии (PhD) по физико-математическим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за №B2022.3.PhD/FM774.

Диссертация выполнена в Национальном Университете Узбекистана имени Мирзо Улугбека.

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

Научный руководитель:	**Жураев Гайрат Умарович** доктор физико-математических наук, профессор
Официальные оппоненты:	**Кабулов Анвар Василович** доктор технических наук, профессор
	Саттаров Алижон Бозорбоевич доктор философии PhD по физико-математическим наукам
Ведущая организация:	**ООО "UNICON.UZ"**

Защита диссертации состоится «07» 11 2025 года в 16[00] часов на заседании Научного совета DSc.03/30.12.2019.FM.01.02 при Национальном университете Узбекистана (Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 227-12-24; факс: (+99871) 246-53-21; e-mail: nauka@nuu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за № 174). Адрес: 100174, г. Ташкент, Алмазарский район, ул. Университетская, 4. Тел.: (+99871) 246-02-24.

Автореферат диссертации разослан «25» октября 2025 года.

(протокол рассылки № 1 от «19» 09 2025 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., профессор

Б.Ф. Абдурахимов
Председатель Научного семинара при научном совете по присуждению ученых степеней, д.ф.-м.н., профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. Многие научные и практические исследования, проводимые в мировом масштабе, посвящены изучению процессов разработки надежных и безопасных ключей в алгоритмах шифрования. Особое внимание уделяется научным исследованиям, направленным на разработку стойких криптографических ключей, улучшение их случайных свойств и повышение их стойкости к анализу ключей. Поэтому создание устойчивых ключей с высокой энтропией, отвечающих современным криптографическим требованиям, остается одной из важных задач криптографии.

В настоящее время в мире широко используются криптографические системы для обеспечения конфиденциальности информации в компьютерных системах. Непосредственная безопасность таких систем тесно связана с стойкостью применяемого в них алгоритма шифрования и конфиденциальностью ключа. Ключ шифрования, как правило, представляет собой последовательность случайных битов, которые генерируются с помощью генератора псевдослучайных чисел (PRNG) или алгоритмов потокового шифрования. Сгенерированные последовательности должны обладать высокой степенью случайности, успешно проходить статистические тесты и быть непредсказуемыми даже при наличии криптоанализа части их исходного или текущего состояния. Поэтому разработка алгоритмов генерации последовательностей с высоким уровнем случайности в современных системах информационной безопасности и использование стойких криптографических ключей при шифровании остается одной из актуальных научно-технических проблем. Поэтому разработка устойчивых криптографически экономичных алгоритмов и определение их эффективности является одним из целевых научных исследований.

В нашей стране особое внимание уделяется научным и прикладным исследованиям в области информационных технологий, информационной безопасности и ее криптографической защиты. Разработка эффективных методов стойких криптографических ключей, повышение их практического применения и обобщения является одной из актуальных задач на сегодняшний день. В результате исследований, проведенных в последние годы, усовершенствованы методы анализа и критерии оценки криптографических алгоритмов, достигнуты важные результаты в дальнейшем развитии национальной системы криптографической защиты информации. Особое внимание уделяется созданию генераторов псевдослучайных чисел по актуальным направлениям развития отечественной криптологии. В обеспечении исполнения решения важное значение имеет разработка раундовых ключей для симметричных блочных алгоритмов шифрования, а также создание алгоритмов потокового шифрования с легким весом и исследование вопросов генерации стойких ключей с их использованием в качестве генератора псевдослучайных чисел.

Данное диссертационное исследование в определенной степени служит выполнению задач, предусмотренных в Законе Республики Узбекистан от 3

апреля 2007 года ПП-614 "О мерах по организации криптографической защиты информации в Республике Узбекистан," Законе Республики Узбекистан от 15 апреля 2022 года ЗРУ-764 "О кибербезопасности," Указе Президента Республики Узбекистан от 28 января 2022 года ПП-60 "О стратегии развития нового Узбекистана на 2022-2026 годы," Постановлении Президента Республики Узбекистан от 31 мая 2023 года ПП-167 "О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан," а также в других нормативно-правовых документах, принятых в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Настоящая работа выполнена в соответствии с приоритетным направлением развития науки и технологий Республики Узбекистан IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Криптографическая защита информационной безопасности, разработка алгоритмов генерации устойчивых криптографических ключей и их оценка с использованием методов криптоанализа исследовались такими учеными, как Б.Шнайер, Н.Фергюсон, Г.Вернам, Т.Зигенталер, А.О.Керкхоффс, Д.Е.Кнут, К.Е.Шеннон, М.Б.Будко, И.И.Слеповичев и другими. За последние несколько лет эти авторы провели множество исследований как с теоретической, так и с практической точки зрения по вопросам защиты информации и разработки алгоритмов.

В нашей республике такие исследователи, как М.М.Арипов, Б.Ф.Абдурахимов, С.К.Ганиев, Д.Е.Акбаров, А.В.Кабулов, О.П.Ахмедова, Г.У.Жураев, Г.Н.Туйчиев, Д.М.Курьязов, А.И.Икрамов, З.Т.Худойкулов, И.Р.Рахматуллаев проводили научные исследования по разработке криптографических алгоритмов защиты информации, симметричных алгоритмов шифрования, хеш-функций, алгоритмов электронной цифровой подписи, а также по созданию аппаратных и программных средств. Однако в настоящее время в нашей республике недостаточно научных исследований, посвященных изучению генераторов псевдослучайных чисел для криптографических нужд.

Связь темы диссертации с научно-исследовательскими работами учреждением высшего образования, где выполнялась диссертация.

Диссертационная работа выполнена в рамках совместного узбекско-индийского прикладного проекта Uzb-Ind-2021-98 «Исследование и разработка алгоритмов потокового шифрования» в соответствии с научно-исследовательским планом Национального университета Узбекистана имени Мирзо Улугбека.

Целью исследования является заключается в разработке устойчивых криптографических ключей с высоким уровнем случайности, соответствующих криптографическим требованиям.

Задачи исследования: разработка алгоритма генерации раундовых ключей для блочных алгоритмов шифрования;

разработка алгоритма потокового шифрования, удобного для реализации в программной форме;

разработка алгоритма потокового шифрования, удобного для реализации в аппаратной форме;

оценка уровня случайности генераторов разработанных алгоритмов шифрования;

оценка устойчивости генераторов ключей разработанных алгоритмов шифрования с использованием методов криптоанализа;

сравнение разработанных алгоритмов потокового шифрования по скорости и характеристикам реализации.

Объектом исследования являются псевдослучайные последовательности с высоким уровнем случайности, которые могут использоваться в качестве криптографических ключей.

Предметом исследования являются алгоритмы потокового шифрования, предназначенные для реализации в аппаратной и программной форме, обеспечивающие генерацию псевдослучайных последовательностей, а также методы оценки их криптографических характеристик.

Методы исследования. В процессе исследования использовались методы криптографии и криптоанализа, дискретной математики, теории вероятностей, теории чисел и объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

разработан алгоритм генерации раундовых ключей для симметричных блочных алгоритмов шифрования, устойчивый к методам криптоанализа;

разработан удобный в программном исполнении алгоритм потокового шифрования, основанный на перемешивании внутренних массивов состояний;

разработан алгоритм потокового шифрования на основе регистров сдвига с нелинейной обратной связью, предназначенный для аппаратной реализации, общей длиной 128 бит и состоящий из 3 регистров сдвига;

разработана гибридная модель криптографического генератора псевдослучайных чисел, обеспечивающая высокий уровень случайности;

разработанные алгоритмы генерации ключей были оценены с использованием методов криптоанализа и доказано, что они устойчивы к атакам более чем в 2^{100} итерациях;

разработанные алгоритмы потокового шифрования сравнивались по скорости реализации, а их криптографическая безопасность оценивалась с помощью статистических тестов.

Практические результаты исследования заключаются в следующем:

разработано программное средство для алгоритма потокового шифрования, удобного для программной реализации;

разработана схема и программное средство для реализации алгоритма потокового шифрования, основанного на регистрах сдвига с линейной обратной связью (LFSR), в аппаратной форме.

Достоверность результатов исследования подтверждается строгостью математических рассуждений, результатами проведенных численных исследований, а также реальными и экспериментальными результатами, полученными при криптоанализе разработанных криптографических алгоритмов.

Научная и практическая значимость результатов исследования.

Научная значимость результатов исследования объясняется возможностью генерации раундовых ключей для симметричных блочных алгоритмов шифрования, алгоритмов генерации ключей в алгоритмах потокового шифрования, удобных для аппаратной и программной реализации, при создании средств криптографической защиты.

Практическая значимость результатов исследования заключается в создании аппаратных и программных средств, предназначенных для генерации ключей на основе алгоритмов потокового шифрования. Они имеют важное практическое значение в обеспечении конфиденциальности и секретности информации в компьютерных системах и сетях и объясняются удобной интеграцией в аппаратной и программной формах.

Внедрение результатов исследования. На основе предложенных алгоритмов и разработанных программных средств получены следующие результаты:

На основе алгоритма AAOOSHA80 (алгоритм потокового шифрования, удобный для аппаратной реализации) в Военном институте информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан разработаны устойчивые криптографические ключи (справка №2648 от 6 ноября 2024 года, Военный институт информационно-коммуникационных технологий и связи Министерства обороны Республики Узбекистан). В результате применения научных результатов достигнута эффективность на 13% по времени шифрования и расшифровки.

Отдельные научные результаты, полученные в диссертации, были использованы в 2021–2023 годах в рамках узбекско-индийского прикладного проекта Uzb-Ind-2021-98 «Исследование и разработка алгоритмов потокового шифрования» на кафедре информационной безопасности Национального университета Узбекистана имени Мирзо Улугбека (справка №04/11-13194 от 16 декабря 2024 года, Национальный университет Узбекистана). На основе разработанного программного средства достигнуто обеспечение конфиденциальности информации при передаче и снижение количества ошибок в процессе передачи.

Апробация результатов работы. Результаты исследования были обсуждены на 5 научно-практических конференциях, включая 2-х международных и 3-х республиканских.

Опубликованность результатов исследования. По теме диссертации опубликовано 14 научных работ, включая 9 статей в научных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан для публикации основных научных результатов диссертаций, из них 4 статьи в зарубежных журналах и 5 статей в республиканских журналах. Также получены 2 свидетельства о регистрации программных средств для ЭХМ.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 112 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** диссертации обосновано актуальность и необходимость темы исследования, показано соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, определены цель и задачи исследования, а также объект и предмет исследования. Обоснована достоверность полученных результатов, их теоретическая и практическая значимость, описано внедрение результатов исследования в практику, представлены сведения о опубликованных работах и структуре диссертации.

В первой главе диссертации под названием «**Использование генераторов псевдослучайных чисел для создания криптографических ключей**», рассматриваются решения задач генерации раундовых ключей для симметричных блочных алгоритмов шифрования с использованием генераторов псевдослучайных чисел. Также обсуждаются вопросы, связанные с алгоритмами потокового шифрования, удобными для реализации в программной и аппаратной форме, существующие в них проблемы и пути их решения.

В §1.1-параграфе анализируются случайные последовательности и их свойства. Безопасность криптографических систем определяется стойкостью используемого в них алгоритма и ключа. Хотя криптографические алгоритмы стабильны, уровень защиты информации при использовании слабого ключа не будет высоким. Согласно принципу Кьеркхоффа, безопасность криптографической системы должна зависеть только от секретного ключа, а алгоритм или метод шифрования должен быть открытым. Кроме того, долговечность ключа зависит от степени случайности составляющих его случайных последовательностей. В частности, для создания последовательности случайных чисел или битов используются устройства, называемые генераторами случайных чисел, и на их основе предоставляются данные. В случайных генераторах энтропия является основной мерой случайности и безопасности.

В случайных генераторах энтропия является основной мерой случайности и безопасности.

Математически энтропия выражается формулой энтропии Шеннона:

$$H(\mathrm{x}) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \qquad (1.1)$$

Используя свойства логарифма H (x), получаем следующую формулу:

$$H(\mathrm{x}) = -\sum_{i=1}^{n} \frac{1}{n}(-\log_2 n) = \log_2 n \qquad (1.2)$$

Если все результаты имеют одинаковую вероятность, то есть максимальную случайность, то энтропия будет наибольшей. Кроме того, если энтропия недостаточна, зашифрованные данные могут быть искажены. Случайные числа являются одним из основных факторов криптографии, и их надежная генерация является основой криптографической безопасности. Описано, что случайные числа, используемые в криптографии, должны иметь высокую энтропию и быть непредсказуемыми.

В §1.2-параграфе в алгоритмах шифрования стороны обмениваются секретным ключом и на его основе генерируется последовательность ключей с помощью ГПСЧ (генератора псевдослучайных чисел).

Сегодня ГПСЧ также широко используются во многих криптографических системах. (Рисунок 1).

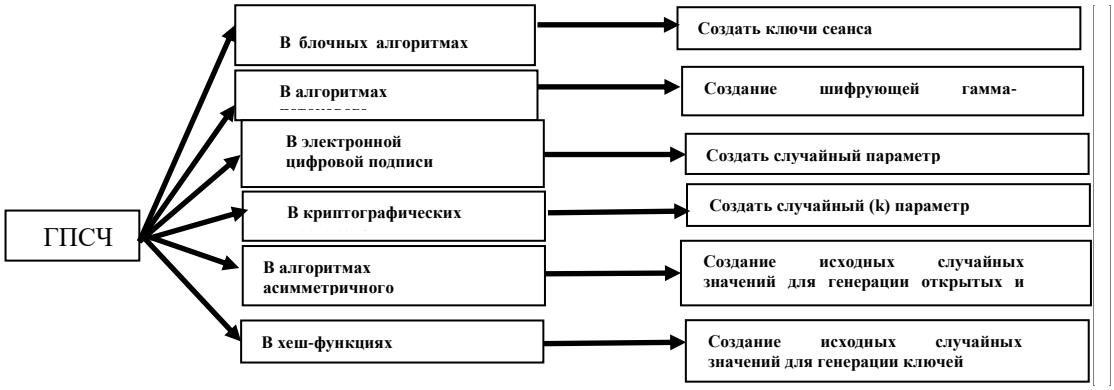


Рисунок 1. Области применения ГПСЧ.

Этот ГПСЧ для криптоанализ методы сделанный увеличивать последовательность узнал и этот анализ методы шифрование алгоритме который слабость к существованию оправдание показано. Также симметрично шифрование алгоритмы с использованием работающий изданный последовательности на волю случая оценка тесты о информация цитируется.

В криптографических системах, использующих секретный ключ, целесообразно использовать ГПСЧ с достаточно большой длиной цикла и высокой степенью случайности. Параметр псевдослучайного генератора $p, k, a_l, a_2, \ldots\ldots, a_k;\ x_{0,}, x_{-l}, \ldots\ldots, x_{-k+1}$. Начальное $\mathrm{x}_0, \mathrm{x}_{-1}, \ldots\ldots, \mathrm{x}_{-\mathrm{k}+1} \in \mathrm{A}$ выбирается произвольно, чтобы одновременно достичь значения 0. Рекуррентный коэффициент $a_l, a_2, \ldots\ldots, a_k \in A$ выбирается таким образом, чтобы полученный многочлен выглядел следующим образом:

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1}x - a_k \qquad (1.3)$$

Теорема 1: Если многочлен k-битового линейного регистра сдвига с обратной связью (LFSR) является примитивным многочленом, то его период имеет максимальную длину $L = 2^k - 1$.

В §1.3-параграфе криптографический безопасный псевдослучайный числа генераторы (ГПСЧ) такие случайный генераторы, из которых взятый случайный чисел абсолютно пророчество как что этого не будет гарантии.

Тест следующего бита ГПСЧ удовлетворяети система ситуации к нарушению против стоит. Требуется безопасность до уровня рассматриваем программирование ГПСЧ поставлять компоненты, аппаратные устройства или их сочетание как сделанный увеличивать возможный. Их функции и выносливость в соответствии с информацией цитируется.

В §1.4-параграфе симметричный блокировать шифрование раунд ключи в алгоритмах анализ и есть течет шифрование алгоритмы анализ сделал. Симметричный шифрование алгоритмы для круглых ключей поколение в соответствии с исследовать достаточно не будучи определенный. Также течет шифрование алгоритмы к приложению особенный интегрированный схема (ASIC) и квадрат программируемый логичный в среде массива (FPGA), программное обеспечение инструмент по внешнему виду сделанный повысился параметров сравнительный анализ результаты стол в виде представлено сделанный. Потоковое вещание шифрование алгоритмы и аппаратное обеспечение программное обеспечение по внешнему виду сделанный увеличить комфортный был течет шифрование алгоритмы создавать и их оценка в соответствии с исследовать достаточно не будучи определенный.

Таблица 1.

Криптостойкость генераторов псевдослучайных чисел анализ свойств.

Название алгоритма	**Длина ключа (bit)**	**Количество включенных операций**	**Производительность**	**Криптостойкость**
Конгруэнтные генераторы	<64	Умножение, mod N	Низкая скорость	$<2^{64}$, с нестойких
Salsa20	128	Сдвиг направо, XOR	Высокая скорость	2^{160}, высокая
ANSI X9.17 FIPS-186 YARROW-160	64-160	Алгоритмы 3DES, 2DES, SHA-1	Низкая скорость, только для создания ключа	2^{128}, высокая
Алгоритм ISAAK	64	Регистр сдвига	Короткий неповторимый период	2^{64}, низкая
A5	64	Комбинация регистров сдвига	Высокая скорость	2^{64}, низкая
RC-4,	до 2048 бит	Mod256, перемещение	Высокоскоростное, имеет патент	2^{64}, низкая
Spritz	до 2048 бит	Mod256, перемещение	Высокая скорость	2^{128}, высокая

Алгоритмы Salsa20 и ANSI X9.17, Spritz обладают высокой криптостойкостью. Алгоритмы, такие как RC4 и ISAAC, считаются уязвимыми, несмотря на высокую скорость.

Во второй главе диссертации под названием **«Методы разработки криптографически стойких ключей»** разработан алгоритм, генерирующий раундовые ключи для алгоритмов симметричного блочного шифрования. Также были разработаны алгоритм потокового шифрования под названием AAOOSHA128 который легко реализовать в аппаратном обеспечении, и алгоритм потокового шифрования под названием MEAG, который основан на непрерывной замене элементов массива, который легко реализовать в программном обеспечении, кроме того, была создана гибридная модель криптографического генератора псевдослучайных чисел.

В §2.1-параграфе предложен алгоритм генерации ключа для симметричных блочных алгоритмов шифрования.

В предложенном алгоритме генерации раундовых ключей изначально используется 256-битный ключ шифрования и 256-битный вектор инсилирования. Секретный ключ K и вектор стремления разделены на 4 части по 64 бита. Признаки этих частей приведены ниже. Алгоритм использует преобразования и константы, в частности, $Rotation$ - функция смещения, S - функция нелинейного преобразования (блок S), R – это функция, которая слагает элементы двух массивов по модулю 2, константы $C_0 \div C_4$ постоянные значения. Сначала посредством нелинейного отображения S заменяет элементы восьми битного массива соответствующими восьми битными значениями из следующего блоке S.

$S = \{182, 99, 75, 57, 194, 175, 102, 209, 192, 180, 244, 230, 210, 116, 166, 89, 82, 108,$
$229, 190, 208, 37, 155, 203, 91, 9, 43, 45, 164, 103, 113, 32, 97, 133, 216, 202, 144,$
$170, 83, 141, 254, 248, 63, 76, 73, 131, 27, 225, 137, 231, 217, 136, 228, 107, 55, 48,$
$247, 29, 172, 134, 64, 179, 88, 7, 59, 149, 213, 105, 125, 165, 163, 140, 47, 85, 94, 39,$
$146, 70, 69, 173, 65, 38, 159, 100, 130, 56, 184, 26, 68, 98, 0, 30, 115, 96, 151, 167, 74,$
$10, 51, 78, 80, 40, 232, 220, 188, 176, 148, 122, 222, 236, 15, 224, 3, 185, 34, 124, 246,$
$214, 121, 215, 201, 67, 168, 62, 169, 36, 245, 223, 87, 13, 189, 195, 128, 198, 84, 109,$
$126, 138, 53, 255, 61, 25, 117, 50, 177, 178, 158, 157, 111, 120, 145, 243, 199, 154, 123,$
$16, 41, 150, 161, 21, 135, 93, 183, 156, 71, 19, 114, 191, 18, 118, 12, 8, 86, 14, 112, 181,$
$204, 206, 58, 253, 162, 104, 42, 242, 171, 72, 200, 234, 81, 44, 52, 235, 31, 211, 212, 127,$
$152, 237, 11, 6, 160, 143, 106, 227, 174, 2, 132, 5, 79, 142, 1, 139, 66, 60, 28, 129, 33, 239,$
$92, 226, 90, 101, 24, 249, 193, 95, 205, 20, 187, 241, 54, 23, 186, 153, 46, 147, 219, 240,$
$119, 233, 77, 4, 197, 35, 218, 250, 196, 251, 22, 49, 110, 207, 17, 252, 221, 238\}.$

Далее, функция замены Rotation, заменяет значения элементов массива состоящих из 64-х битов следубщим образом: $a_0, a_1, \ldots, a_7$ соответственно a_0, массив не сдвигается, a_1массив сдвигается на 1 бит, a_2массив сдвигается на 2 бита и т. д., a_7 массив сдвигается циклически на 7 бит. После этого,a_7 множество на душу населения оставшийся массивы один байт десять выталкивается.

$$a_0 = a_0$$
$$a_1 = a_1 \lll 1$$
$$a_2 = a_2 \lll 2$$
$$a_3 = a_3 \lll 3$$
$$a_4 = a_4 \lll 4$$
$$a_5 = a_5 \lll 5$$
$$a_6 = a_6 \lll 6$$
$$a_7 = a_7 \lll 7$$
$$\{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \rightarrow \{a_7, a_0, a_1, a_2, a_3, a_4, a_5, a_6\}.$$

В результате, при генерации ключей шифрования для n раундов рассчитывается $N = 4 * (n + 1)$ состоящих из шагов $(i = 1,2, \ldots, n)$ с использованием следующих формула

$$k_i = S\left(R\left(S\left(R(R(k_{i-4}, C_{i \bmod 4}), iv_{i \bmod 4})\right), Rotation(k_{i-1})\right)\right), i \bmod 4 \neq 0; \quad (2.1)$$

$$k_i = R(S(k_{i-1}), k_{i-4}), \ i \bmod 4 = 0; \quad (2.2)$$

при формировании ключей из $i = 0,1, \ldots, n$ раундов, сформированные элементы массива k_i могут использоваться в любой и уникальной последовательности.

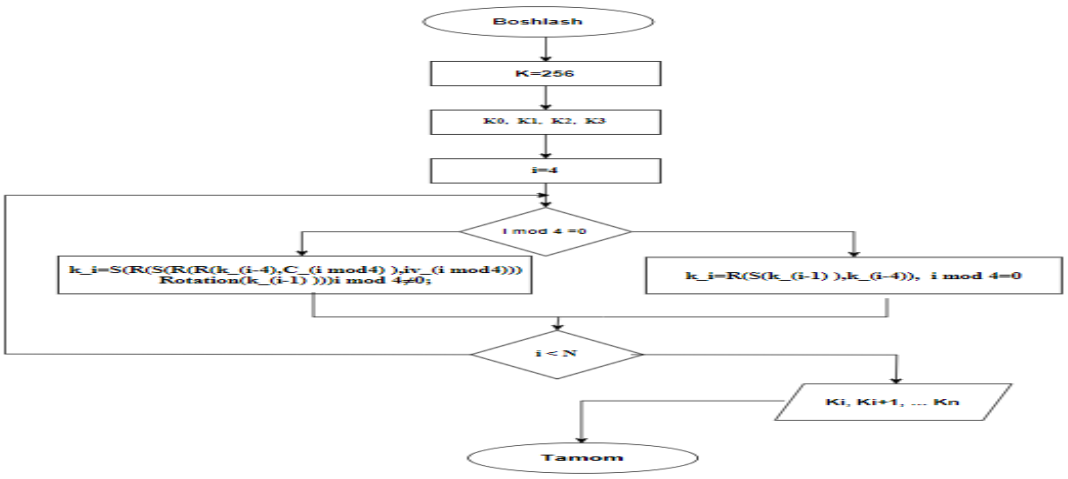


Рисунок. 2. Блок-схема алгоритма генерации раундовых ключей.

Утверждение 1. Алгоритм генерации раунддовых ключей для симметричных блочных алгоритмов шифрования, основанных на операциях нелинейного преобразования и циклического сдвига, обеспечивает высокую случайность.

В §2.2-параграфе начальное состояние AAOOШA128 (Аппаратно реализованный алгоритм потокового шифрования) строится из 3 регистров сдвига по 47, 40 и 41 бит, общей длиной 128 бит. Каждое состояние изменяется посредством комбинации нелинейной передачи и обратной связи битов в правых регистрах циклического сдвига. Для инициализации шифра секретный ключ К длиной 128 бит записывается в 3 регистра сдвига в соответствии с заданным правилом, а процесс инициализации выполняется за 40*41 = 1640 итераций, что гарантирует, что каждый бит начального состояния связан с каждым битом ключа. Он состоит из 7 элементов И и 18 элементов исключающее или.

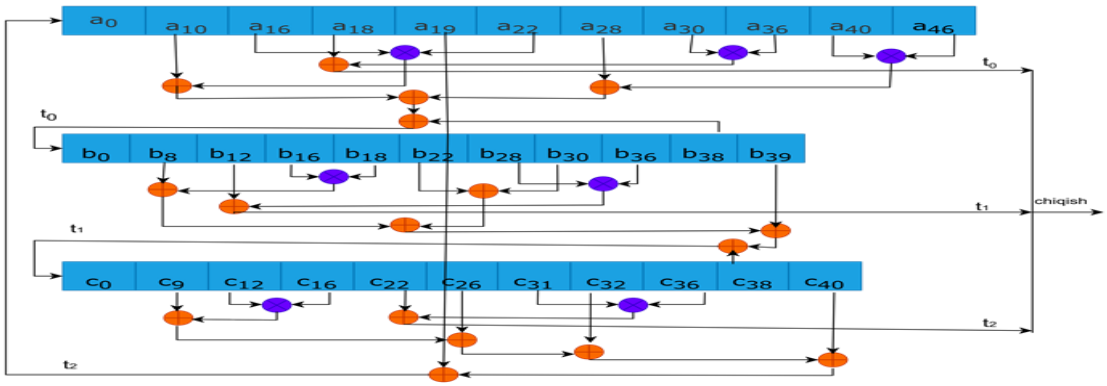


Рисунок. 3. Функциональная схема алгоритма AAAOOSHA128 .

Алгоритм реализуется путем сложения 128-битного ключа с 128-битным вектором инициализации по модулю 2 б, создавая 128 (47+40+41)-битных регистров начального состояния, как показано в следующем псевдокоде.

$$K = K \oplus IV$$
$$(K_0, K_1, \dots, K_{46}) \rightarrow (a_0, a_1, a_2, \dots, a_{46})$$
$$(K_{47}, K_{48}, \dots, K_{86}) \rightarrow (b_0, b_1, b_2, \dots, b_{39})$$
$$(K_{87}, K_{88}, \dots, K_{127}) \rightarrow (c_0, c_1, \dots, a_{40})$$
$$for\ i = 0\ to\ 1640\ do$$

$$a_{10} \oplus a_{16} \cdot a_{22} \oplus a_{28} \oplus a_{40} \cdot a_{46} \oplus b_{38} \to t_0$$
$$b_8 \oplus b_{16} \cdot b_{18} \oplus b_{22} \oplus b_{30} \oplus b_{39} \oplus c_{38} \to t_1$$
$$c_9 \oplus c_{12} \cdot c_{16} \oplus c_{26} \oplus c_{32} \oplus c_{40} \oplus a_{19} \to t_2$$
$$(t_2, a_0, \dots, a_{45}) \to (a_0, \dots, a_{46})$$
$$(t_1, b_0, \dots, a_{38}) \to (b_0, \dots, b_{39})$$
$$(t_0, c_0, \dots, c_{39}) \to (c_0, \dots, c_{40})$$
$$end\ for.$$

AAOOSHA128 внутренний статус обеспечить регресс в некотором роде будет обновлено, а инициализация регистра ($c_0, .., c_{40}$) предотвращает цикличность состояния менее чем за 40 итераций. Для обеспечения в алгоритме генерации псевдослучайных последовательности используется уравнение обратной связи:

$$s(t+1) = (a_1 s(t) \oplus a_2 s(t-1) \oplus \dots \oplus a_n s(t-n+1)) \bmod 2 \qquad (2.3)$$

здесь: $s(t)$- состояние в момент времени t , $a_и$- коэффициенты обратной связи ($a_и \in \{0,1\}$).

В качестве функций обратной связи обычно используют примитивные многочлены. Свойство характерного многочлена f(x) можно оценить с примитивным многочлен со степенью k, это определяется следующим образом: примитивный многочлен порядка f(x) называется многочленом со степенью k, если задано $f(x) = \sum_{i=0}^{n} a_i x^i, n > k,\ a_i \in GF(2), i = 0,1, \dots, n$ и $f(x) = (x+1)^k \cdot g(x)$, здесь - $g(x)$ также будет примитивным многочленом. Биты показанные в индексах f(x) суммируются по модули 2 и получается новый бит следующим образом:

$$s_{n+1} = s_{n-132} \oplus s_{n-129} \oplus s_{n-123} \oplus \cdots \oplus s_{n-3} \oplus s_n \qquad (2.4)$$

В результате индексы битов, соответствующие каждой степени в многочлене f (x), можно записать следующим образом:

$$f(x) = x^{132} + x^{129} + x^{126} + x^{120} + x^{114} + x^{108} + x^{87} + x^{75} + x^{72} + x^{63} + x^{60} + x^{57} + x^{54} + x^{48} + x^{45} + x^{33} + x^{27} + x^{21} + x^{12} + x^9 + x^6 + 1$$

Теорема 2: Если характеристический многочлен алгоритма AOOSHA128 имеет вид $f(x) = (x^3+1)^3 \cdot g(x^3)$, то многочлен $f(x)$ является примитивным многочленом третьего порядка.

Результатом расчета является криптографический PRNG или поточный бит шифрования.

Утверждение 2. Если алгоритм поточного шифрования ААООША128 оптимизирован для аппаратной реализации, тогда обеспечивается высокая безопасность и эффективность на основе регистров сдвига нелинейной обратной связи и примитивных многочленов.

В результате становится возможным генерировать ключи длиной до 2^{64} бит с использованием 128-битного секретного ключа, что обеспечивает максимальную надежность сгенерированных ключей.

В §2.3-параграфе предлагается алгоритм потокового шифрования, удобный для реализации в программном виде. Процесс создания ключей в MEAG (генератор, переключающий элементы массива), аналогичен RC4, но основан на непрерывном переключении элементов массива с дополнительной сложностью, которые введены вспомогательными

переменными. Основная процедура алгоритма как потокового шифрования состоит из трех процессов: алгоритма планирования ключей (KSA), алгоритма псевдослучайного генерации (PRGA) и процесса шифрования или дешифрования.

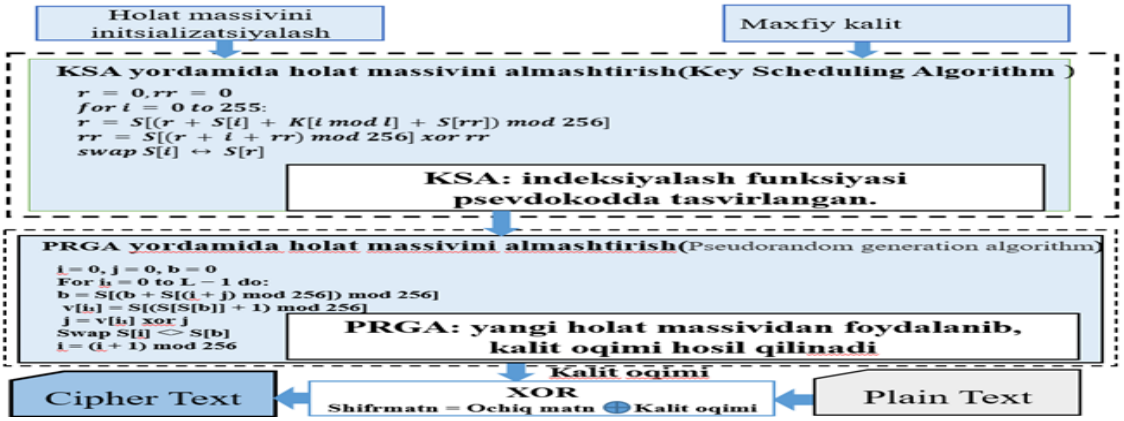


Рисунок. 4. Схема работы генератора MEAG.

Процесс планирования ключей (KSA) состоит из инициализации массива S-Бох (S) из 256 элементов и преобразования его в алгоритм, зависящий от ключа (PRGA). В нем массив S имеет 256 ячеек. Процесс обмена управляется через индексы r, rr и i. На этапе PRGA процесс шифрования происводится с помощью последовательной генерации байтов и получается поток ключей. На каждой итерации индексы i, j, b будут обновлены внутри алгоритма и в массиве S происходит динамический обмен элементов. С помощью генератора подстановки элементов массива выполняется операция сложения зашифрованного текста по модулю 2 ключом дешифрования зашифрованных данных (рис. 5).

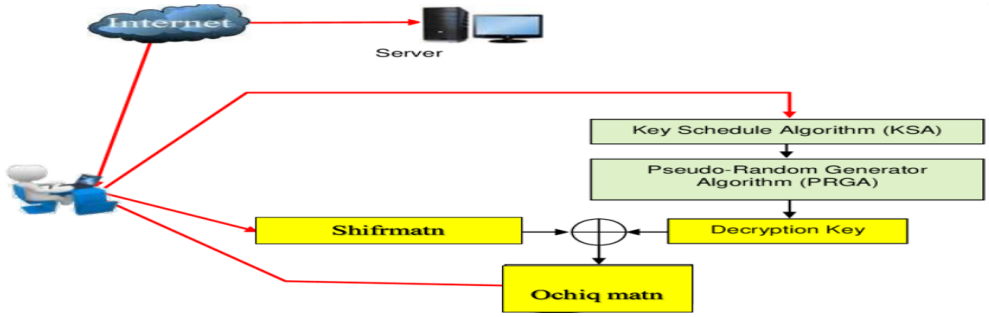


Рисунок. 5. Схема алгоритма MEAG.

Алгоритм MEAG считается очень надежным в процессе случайной генерации ключей, требуя небольшого времени для шифрования и дешифрования. В RC4 обнаружены атаки методом перебора и прямого перебора во время шифрования и дешифрования в алгоритме MEAG. Он считался устойчивым к атакам Флэрера-Мантина-Шамира.

Утверждение 3. Если алгоритм MEAG основан на динамическом преобразовании элементов массива и нелинейных преобразованиях, то обеспечивается более высокая безопасность по сравнению с алгоритмом RC4. В §2.4-параграфе один из генераторов ГПСЧ, основанный на методе регистров сдвига с обратной связью, представляет особый интерес благодаря

быстродействующей последовательности "средний квадрат Вейля." Псевдослучайный генератор Вейля - это алгоритм, который использует квадратичные и модульные операции для генерации последовательности случайных чисел.

$$w_{i+1} = w_i + c,$$
$$x_{i+1} = x_и^{\,2} + w_{i+1},$$
$$y_{i+1} = (x_{i+1} \text{ мод } 2^{64}) \gg 32, \qquad (2.5)$$

Для защиты слабых сторон алгоритма Вейля предлагается использовать гибридную версию ГПСЧ, по следующей схеме. Вводится двухсекционный ключ, в котором регистр сдвига с обратной связью строится из треугольной конструкции нижеследующего типа. Этот процесс показан на рис. 7.

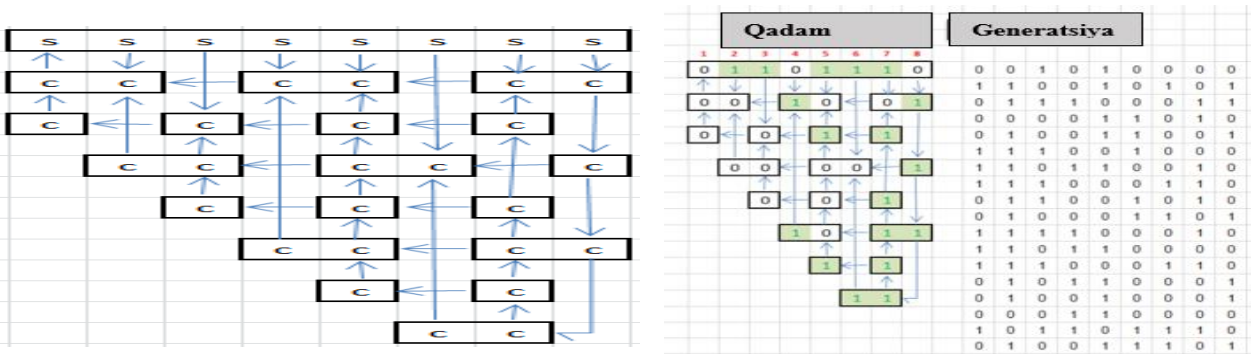


Рисунок. 7. Треугольная конструкция регистра перемещений с обратной связью.

Модель структуры S создает базовую структуру памяти , а структура ***c*** описывает работу генератора псевдослучайных чисел в зависимости от памяти S. Длина этой последовательности случайных чисел зависит не только от количества цифр, но и от состояния внутренних регистров с.

$$M \approx 2^{0,35*n^2+n}, \qquad (2.6)$$

где n – количество разрядов. M – длина цикла случайности. Чем меньше длина цикла, тем быстрее выполняется итерация ГПСЧ. Отличительной особенностью программной реализации регистра обратной связи является то, что ячейки могут содержать не только битовые значения, но и другие значения, не превышающие « n/2 », например, от 0 до 3 (рис. 8).

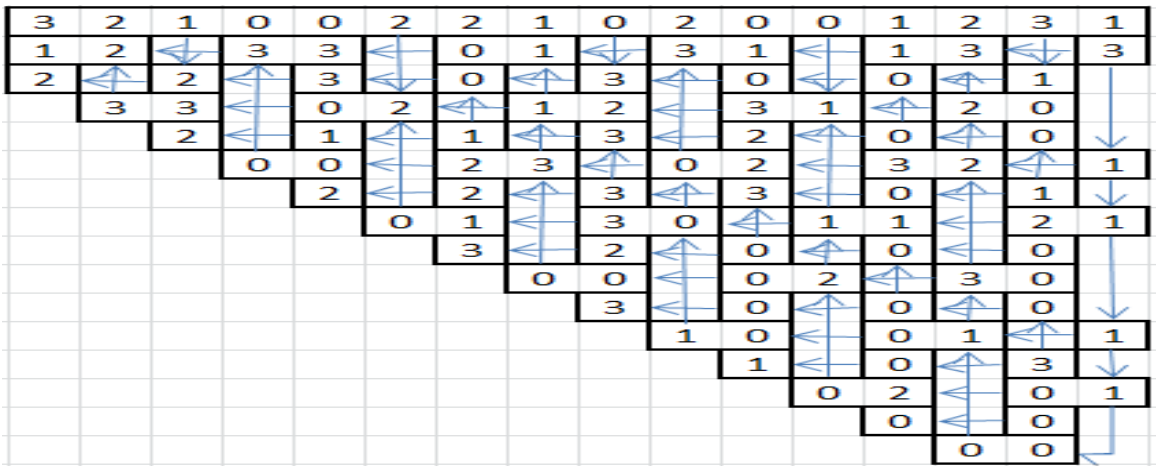


Рисунок. 8. Изменение регистра с обратной связью цифр от 0 до 4^{16}.

Для увеличения периодичности гибридной модели значение M можно изменить следующим образом.

$$M \approx c^{0,35*n^2+n} \quad (2.7)$$

Общий вид предлагаемой гибридной модели выглядит следующим образом.

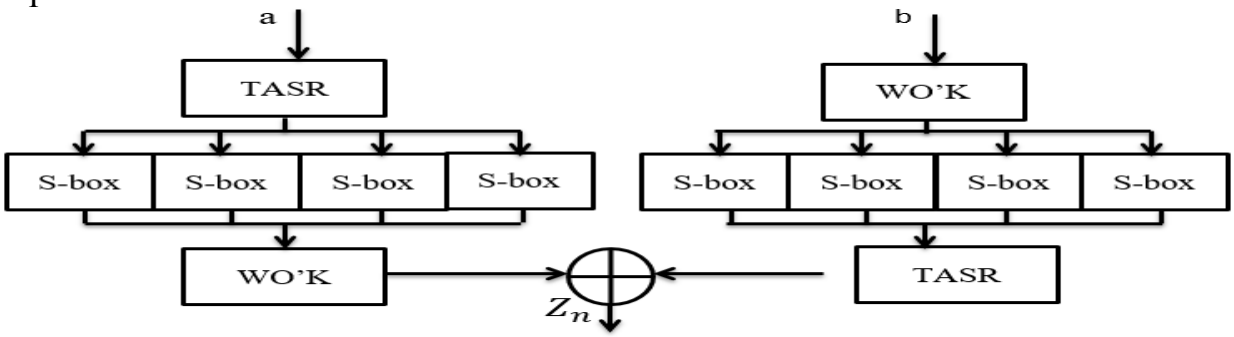


Рисунок. 8. Общая схема гибридного ГПСЧ.

Последовательности, полученные из псевдослучайных чисел, сгенерированных регистрами сдвига с обратной связью (ФСР) и потоком среднеквадратичного распределения Вейля (WMC ***),*** меняются местами при прохождении S-блока**.** После этого он рассчитывается путем сложения 2 модулей. В результате гибридный ГПСЧ выглядит как следующее математическое выражение:

$$Z_n = Y_n\left(S(\sum_{i=0}^{L-1} c_i \cdot X_{n-i} \text{ мод} 2)\right) \oplus X_n\left(S\left((Y_n + w)\text{мод}c^{0,35*n^2+n}\right)\right) \quad (2.8)$$

В этой модели к схеме генерации случайных чисел добавляется нелинейная функция, два типа шифрования дополняют друг друга, а выходная гамма исключает возможность анализа внутреннего состояния системы.

Утверждение 4. Гибридная модель ГПСЧ, основанная на регистрах сдвига с обратной связью и последовательности среднего квадрата Вейля, обеспечивает высокую случайность и криптографическую безопасность посредством нелинейных функций.

В третьей главе диссертации «**Оценка и сравнение разработанных криптостойких ключей с использованием методов криптоанализа**» приведены результаты оценки алгоритма генерации раундовых ключей для симметричных блочных алгоритмов шифрования, а также методов криптоанализа алгоритмов потокового шифрования, удобных для аппаратной и программной реализации.

В §3.1-параграфе приводятся оценки предложенных алгоритмов на тестах случайности. В NIST каждый один поэтапно тест расчет через p - значение найдено. Полученный результаты через последовательность от тестирования пройдено не пройдено определяется. Если значение p находится в диапазоне [0,1] если от тестирования прошлое будет.

Алгоритм генерации ключей раунда был реализован с помощью статистических тестов NIST (табл. 2).

Таблица 2

Результаты оценки статистического теста NIST

Название теста	Результат (p-значение)	Состояние	Успешный диапазон
monobit_test	0.8975605639	PASS	0.01-0.99
frequency_within_block_test	0.2708842358	PASS	0.01-0.99
runs_test	0.5036686676	PASS	0.01-0.99
longest_run_ones_in_a_block_test	0.9553989385	PASS	0.01-0.99
binary_matrix_rank_test	0.2201007292	PASS	0.01-0.99
dft_test	0.3752687226	PASS	0.01-0.99
non_overlapping_template_matc hing_test	0.9999648101	PASS	0.01-0.99
overlapping_template_matching_ test	0.5733547337	PASS	0.01-0.99
maurers_universal_test	0.0987345585	PASS	0.01-0.99
linear_complexity_test	0.7387164598	PASS	0.01-0.99
serial_test	0.8419852083	PASS	0.01-0.99
approximate_entropy_test	0.8818725039	PASS	0.01-0.99
cumulative_sums_test	0.6144715890	PASS	0.01-0.99
random_excursion_test	0.2025454198	PASS	0.01-0.99
random_excursion_variant_test	0.0194967674	PASS	0.01-0.99

В алгоритме AAOOSHA128 также оценивался уровень случайности последовательностей, сгенерированных с помощью вышеуказанного ключа, с помощью статистических тестов NIST. Результаты оценки показали хороший результат. Ниже на рис. 9 представлены приблизительный энтропийный тест и результаты, полученные по 15 тестам.

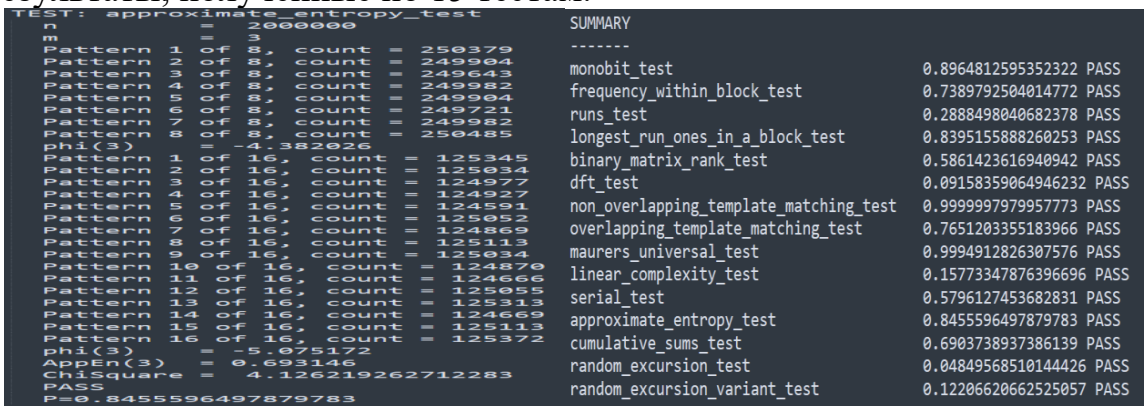


Рисунок. 9. Результаты оценки алгоритма AAOOSHA128 с помощью статистического теста NIST

Случайные результаты предложенного алгоритма MEAG по 1000000 битам, зашифрованным с использованием теста NIST, представлены в таблице

Таблица 3

Результат статистического теста NIST алгоритма MEAG

Название теста	Результат	Состояние	Успешный диапазон
monobit_test	0.881368	Pass	0.01-0.99
frequency_within_block_test	0.781296	Pass	0.01-0.99
runs_test	0.596638	Pass	0.01-0.99
longest_run_ones_in_a_block_tes t	0.752839	Pass	0.01-0.99
binary_matrix_rank_test	0.860583	Pass	0.01-0.99
dft_test	0.639160	Pass	0.01-0.99
non_overlapping_template_matc hing_test	0.691478	Pass	0.01-0.99
overlapping_template_matching _test	0.224202	Pass	0.01-0.99
maurers_universal_test	0.805704	Pass	0.01-0.99
linear_complexity_test	0.117861	Pass	0.01-0.99
serial_test	0.597103	Pass	0.01-0.99
approximate_entropy_test	0.809020	Pass	0.01-0.99
cumulative_sums_test	0.876226	Pass	0.01-0.99
random_excursion_test	0.914524	Pass	0.01-0.99
random_excursion_variant_test	0.985330	Pass	0.01-0.99

В §3.1-параграфе приведены результаты оценки криптостойкости предложенных алгоритмов методами криптоанализа. Первые алгоритмы симметричного блочного шифрования выводили линейные алгебраические уравнения для однобитной операции циклического сдвига, используемой в раундовых ключах.

$$y_0 = x_7 \oplus x_6x_5x_4 \oplus x_3x_2x_1 \oplus x_0$$
$$y_1 = x_7x_6x_5 \oplus x_4x_3x_2 \oplus x_1x_0$$
$$y_2 = x_7x_6x_5x_4x_3 \oplus x_2x_1x_0 \oplus x_7$$
$$y_3 = x_7x_6x_5 \oplus x_4x_3x_2x_1 \oplus x_0x_7x_6$$
$$y_4 = x_7x_6x_5x_4 \oplus x_3x_2x_1x_0 \oplus x_6x_4x_2$$
$$y_5 = x_7x_6x_5x_4x_3 \oplus x_2x_1x_0x_7x_6 \oplus x_4x_3$$
$$y_6 = x_7x_6x_5x_4x_3x_2 \oplus x_1x_0x_7x_5 \oplus x_4x_2x_1$$
$$y_7 = x_7x_6x_5x_4x_3x_2x_1 \oplus x_0x_7x_6x_5 \oplus x_4x_3x_2$$

После формирования алгебраических уравнений для каждой перестановки, путем их объединения формируются уравнения для одного раунда. Результат представляет параметры уравнений, построенных с использованием метода алгебраического криптоанализа для генерации раундовых ключей.

Таблица 4.

Параметры уравнений, сформулированных методом алгебраического криптоанализа для алгоритма

Итерация	Изменяемость неизвестных чисел	Сложность числа равно $O(n^3)$
2	2^{14}	2^{42}
3	2^{16}	2^{48}
4	2^{20}	2^{60}
5	2^{22}	2^{66}
6	2^{42}	2^{126}
7	2^{44}	2^{132}
8	2^{48}	2^{144}
9	2^{50}	2^{150}
10	2^{88}	2^{264}

В этой таблице можно сделать вывод, что алгоритм генерации раундовых ключей относительно устойчив к алгебраическому криптоанализу из-за сложности решения, начиная с 7 итераций процесса инициализации. Результаты оценки криптостойкости предложенного алгоритма как с помощью методов линейного, так и дифференциального криптоанализа представлены в таблице

Таблица 5.

Оценка методами криптоанализа

Алгоритм	Алгоритм генерации раундовых ключей
Алгебраический криптоанализ	В 7-й итерации инициализации цикла генерирует сложность 2^{132}
Дифференциальный криптоанализ	После 6-й итерации цикла инициализации дифференци-альная вероятность падает на 2^{-414} уровня. Дифференциал становится устойчивым к криптоанализу.
Линейный криптоанализ	На итерации 7 невозможно определить линейный анализ, когда 2^{-8}

В таблице 6 представлены результаты параметров уравнения, сформулированные методом алгебраического криптоанализа алгоритма AAOOША128.

Таблица 6.

Оценка алгоритма AAOOSHA128 методом алгебраического криптоанализа

Минимальный уровень системы уравнений	Шаг итерации	Число неизвестны	Сложность $O(n^3)$
Уровень 2	47	2^7	2^{21}
Уровень 3	47+40=87	2^{14}	2^{21}
Уровень 4	87+41=128	2^{21}	2^{63}
Уровень 5	128+47=175	2^{28}	2^{84}
Уровень 6	175+40=215	2^{35}	2^{105}
Уровень 7	215+41=256	2^{42}	2^{126}
Уровень 8	256+47=303	2^{49}	2^{147}

В процессе инициализации алгоритма шифрования AOOSHA128, резкое увеличение числа неизвестных переменных после 303-й итерации (2^{49}) и высокая сложность решения этой системы уравнений (2^{147}) позволяют сделать вывод о том, что данный алгоритм устойчив к алгебраическим методам криптоанализа. Исходя из вышеизложенных результатов, результаты оценки методов криптоанализа алгоритмов Trivium и AAOOSHA128 представлены в таблице 3.6.

Таблица 7.

Оценка алгоритма AAOOSHA128 методами криптоанализа

Алгоритм	Trivium	AAOOШA128
Алгебраический криптоанализ	Инициализация в 325-й итерации цикла $2^{42,2}$ неизвестно	Инициализация в -256-й итерации цикла 2^{42} неизвестный
Дифференциал криптоанализ	2^{129} Инициализация после 961-й итерации цикла прочный	Инициализация после 412-й итерации цикла прочный
Линейный криптоанализ	неизвестных в 564-й итерации цикла инициализации	2^{129} неизвестных в 337-й итерации цикла инициализации

Анализ результаты Trivium алгоритм с в сравнении криптоанализ результаты, предложение сделанный Алгоритм AAOOSHA128 достаточно безопасность до уровня имеет что показал.

В §3.3-параграфе разработанные алгоритмы оцениваются по скорости и характеристикам реализации. Представлена процедура аппаратной реализации алгоритма AAOOSHA128 и представлены полученные результаты от них. В программе Proteus реализована схема аппаратной реализации алгоритма AAOOSHA128 (рис.10).

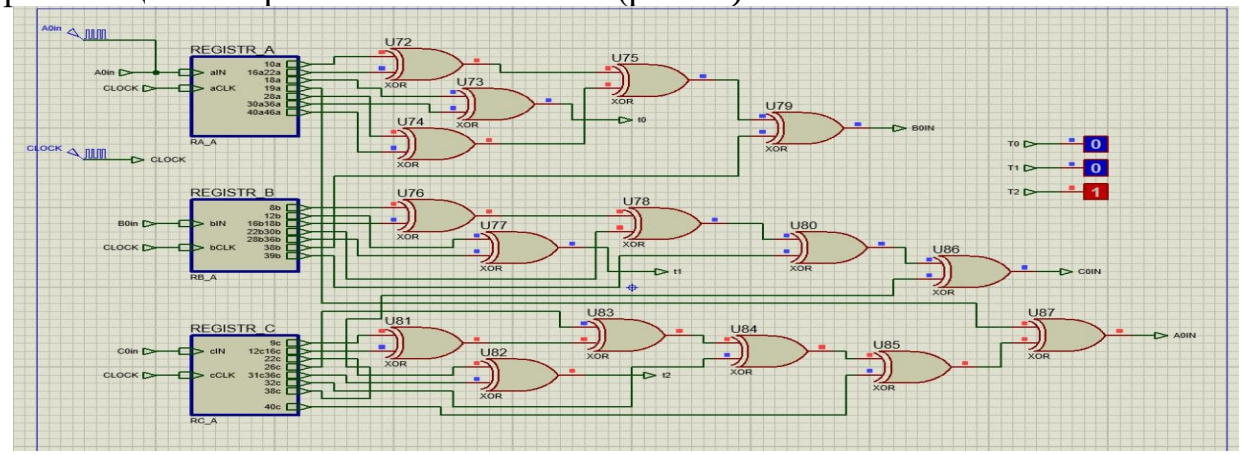


Рисунок. 10. Общая схема аппаратной реализации алгоритма AAOOSHA128

В таблице 8. представлены алгоритмы потокового шифрования, участвовавшие в конкурсе eStream, удобные для аппаратной реализации, и параметры аппаратной реализации алгоритма AAOOSHA128.

Таблица 8.

Анализ алгоритма AAOOSHA128 и других потоковых алгоритмов по случайности и скорости.

№.	Алгоритм имя	Особенный тесты наборы основано на анализ результат (из 15 тестов)	Скорость (Мбит/с)
1.	Salsa20	15	450
2.	Cha-Cha	15	470
3.	HC-128	15	378
4.	HC-256	15	490
5.	ISAAK	15	415
6.	AES-CTR 128	15	478
7.	NSA	15	330
8.	AAOOSHA128	15	342

Результаты анализа, предложенного алгоритма AAOOSHA128 в статистическом тесте NIST состоит из 15. Метод шифрования алгоритма AAOOSHA128 составил 342 Мбит/сек.

Факторный анализ результатов реализации алгоритма MEAG в программном виде в среде программирования приведена в таблица 3.8, в котором также показан, в каком случае получается хороший показатель.

Таблица 9.

Факторный анализ алгоритмов в среде программирования

Шир	Длина ключа (бит)	IV (бит)	Запуск (цикл)	Шифрование (цикл)	RAM (Кбайт)	ROM (Кбайт)	Пропускная способность (MBps)	СМ
Хороший			Низкий	Низкий	Низкий	Низкий	Высокая	Низкий
Enocoro	128	64	512	1024	1.2	3.8	5.1	226
Salsa20	256	64	460	1024	2	5	9.7	278
HC-128	128	128	770	1536	2.5	4	7.9	262
AES-CTR	128	–	1024	2048	3	5	4.95	355
Spritz	128	–	256	1024	1.5	2.5	10.1	350
RC4	256	–	1024	2048	2	3	8.6	210
MEAG	256	–	512	1536	1.8	2.8	10.3	203

Алгоритм потокового шифрования MEAG, удобный для реализации в виде программных средств, отличается от остальных своей скоростью и коротким временем запуска. В частности, алгоритм MEAG может быть использован в ИОТ аппаратах на основе безопасности, скорости и низкого ресурсопотребления.

ЗАКЛЮЧЕНИЕ

В соответствии с целью и задачами, поставленными в диссертационной работе, были получены следующие результаты:

1. Разработан алгоритм генерации раундовых ключей для симметричных блочных алгоритмов шифрования. Разработанный алгоритм позволил производить надежные раундовые ключи даже при внесении изменений.

2. Разработан алгоритм потокового шифрования, предназначенный для аппаратной реализации. Разработанный алгоритм состоит из 3 регистров сдвига общей длиной 128 бит. Алгоритм AAOOSHA128 при реализации на аппарате потребовал на 1893 меньших GATE, чем алгоритм Trivium.

3. Разработан алгоритм потокового шифрования, основанный на замене элементов массива. Разработанное программное средство позволило достичь эффективности 13% по времени шифрования и преобразования в исходный текст.

4. В результате анализа алгоритм генерации раундовых ключей показал устойчивость к алгебраическому методу криптоанализа после 8-й итерации, линейному криптоанализу после 6-й итерации и дифференциальному криптоанализу после 7-й итерации. В результате анализа была определена устойчивость алгоритма поточного шифрования AAAOOSHA128 к алгебраическим, линейным и дифференциальным методам криптоанализа.

5. Разработанные алгоритмы потокового шифрования проанализированы по скорости и особенностям реализации. Согласно результатам анализа, предложенный алгоритм потокового шифрования AAAOOSHA128 имеет результат 15 в наборах статистических тестов NIST, а скорость составляет 342.65 Мбит/сек.

6.Алгоритм MEAG - это упрощенный программный алгоритм, основанный на ключах, который можно использовать на устройствах интернета вещей (IoT). Его можно будет использовать на устройствах, требующих безопасность, скорость и меньших ресурсов.

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

BOZOROV ASQAR XAITMUROTOVICH

DEVELOPMENT OF ROBUST CRYPTOGRAPHIC KEYS

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

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON PHYSICS AND MATHEMATICS SCIENCES

Tashkent-2025

The theme of dissertation of doctor of philosophy (PhD) on physical and mathematical sciences was registered at the Supreme Attestation Commission at the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan under number B2022.3.PhD/FM774.

The 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.nuu.uz and on the website of «ZiyoNet» Information and educational portal www.ziyonet.uz.

Scientific adviser:	**Juraev Gayrat Umarovich** Doctor of Physical and Mathematical Sciences, Professor
Official opponents	**Kabulov Anvar Vasilovich** Doctor of Technical Sciences, Professor
	Sattarov Alijon Bazarbayevich Doctor of Philosophy in Physical and Mathematical Sciences, PhD
Leading organization:	**UNICON.UZ LLC**

Defense will take place "07" 11 2025 at 16^{00} 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, Tel.: (+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 №174) (Address: University str. 4, Almazar area, Tashkent, 100174, Uzbekistan, Tel.: (+99871) 246-02-24).

Abstract of dissertation sent out on "25" October 2025 year.

(Mailing report № 1 on "19" 09 2025 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.

B.F. Abdurakhimov
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 development of robust cryptographic keys that meet cryptographic requirements and have a high degree of randomness.

The object of the research work. Pseudorandom sequences with a high degree of randomness, which can be used as a cryptographic key.

The scientific novelty of the research work: an algorithm for generating round keys for symmetric block encryption algorithms, resistant to cryptanalysis methods, has been developed;

a stream cipher algorithm based on the mixing of internal state arrays has been developed, which is convenient for software implementation;

a hardware-based flow encryption algorithm based on shift registers with nonlinear feedback, with a total length of 128 bits and consisting of 3 shift registers, has been developed;

a hybrid model of a cryptographic pseudorandom number generator has been developed, providing a high degree of randomness;

The developed algorithms for generating keys were evaluated using cryptanalysis methods and proved their resistance to attacks in more than 2^{100} iterations;

the developed flow encryption algorithms were compared in terms of implementat ion speed, and their cryptographic security was assessed using statistical tests.

Implementation of the research results. Based on the results obtained from

the proposed algorithms and software tools developed based on them:

a stable cryptographic key was developed at the Military Institute of Information and Communication Technologies and Communications based on the software-enabled AAOOSHA80 (a stream cipher algorithm that is easy to implement on the device) (Certificate of the Military Institute of Information and Communication Technologies and Communications of the Ministry of Defense of the Republic of Uzbekistan No. 2648 dated November 6, 2024). As a result of the application of scientific results, an efficiency of 13% in terms of encryption and decryption time was achieved.

Some of the scientific results obtained in the dissertation work were used in the joint Uzbek-Indian practical project Uzb-Ind-2021-98 "Research and development of stream cipher algorithms" carried out in 2021-2023 at the Department of Information Security of the National University of Uzbekistan named after Mirzo Ulugbek. (National University of Uzbekistan, 2024, 16

Structure and volume of the dissertation. The dissertation consists of an introduction, four chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 112 pages.

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

I bo‘lim (I часть; I part)

1. Juraev G.U., Bozorov A.X., Sindorov D.S., Salimov S.M. Key Generation Algorithm based on Array Element Substitution // International Journal of Engineering Trends and Technology. – 2024. – T. 73. – №. 4. – C. 224–229. (3, Scopus IF=0.162)

2. Juraev G.U., Raximberdiyev Q.B., Abdullayev T.R and Bozorov A.X. Mathematical modeling of key generators for bank lending platforms based on blokchain technology. Artificial Intelligence Blockchain Computing and Security Volume 2, , 2023, 741-749. (3, Scopus)

3. Juraev G.U., Bozorov A.X and Boykuziev I. Round key formation algorithm for symmetric block encryption algorithms. E3S Web of Conferences 501, 02007/2024 (3, Scopus)

4. Juraev G.U., Bozorov A.X. Protection of transaction data of financial information systems in communication networks based on Sea80's new stream encryption algorithm. NEW2AN 30 july 2025. 62-67 pp. (3, Scopus)

5. A.X. Bozorov. Kriptografik kalitlar ishlab chiqishda psevdotasodifiy sonlar generatorlarini qo’llash Namangan Davlat universiteti ilmiy axborotnomasi // Jurnal, 2022-yil, dekabr 12 soni, 18-23 b. (05.00.00; OAK Rayosatining 2019-yil 28-fevraldagi 262/9.2-son qarori).

6. Bozorov A.X. Apparatda amalga oshiriladigan SEA128 yangi oqimli shifrlash algoritmi. ILM SARCHASHMALARI ilmiy-nazariy metodik jurnali, 2024-yil, 9-son, B. 18–24. (05.00.00; №12)

7. Bozorov A.X. Using effective cryptographic keys to protect information. O‘zMU xabarlari, Maxsus son, 2023-yil, B. 67–71. (01.00.00; №8)

8. Juraev G.U., Bozorov A.X., Ikramov A.A., Farmonov B.D. Нелинейные регистры сдвига. Ахбороткоммуникациялар: тармоқлар – технологиялар – ечимлар, 2(66),2023, 66-71. (05.00.00; №2)

9. Juraev G.U., Bozorov A.X., Farmonov B.D. Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью и линейные регистры сдвига. Ҳарбий таълим ва фанда инновациялар, 2022-yil, 3-son, B. 12–15. (05.00.00; №34)

II bo‘lim (II часть; II part)

10. Bozorov A.X, Muhammadiyev F.R “Bardoshli kriptografik kalitlarni yaratishda psevdotasodifiy raqamlar generatorlaridan foydalanish” International scientific journal science and innovation special issue “digital technologies. Tashkent, 27 - 28 Aprel. 2023 y.

11. Bozorov A.X. Massiv elementlarini almashtirishga asoslanga kalit generatsiya algoritmi. Harbiy aloqa instituti, Respublika ilmiy va amaliy konfereniyasi Tashkent, 27 - 28 Noyabr. 2024 y.

12. Raximberdiyev Q.B., Bozorov A.X., Berdimurodov M.A. Raund key generation algorithm used in symmetric block encryption algorithms to ensure the security of economic systems. International Conference on Future Networks and Distributed Systems, ICFNDS 2024.

13. Bozorov A.X. Psevdotasodifiy ketma-ketlik generatorining matematik asoslari va dasturiy ta’minoti. O‘zbekiston Milliy universiteti talabalar va ilmiy-tadqiqotchilarining ilmiy konferensiyasi” mavzusidagi ilmiy-amaliy anjuman. O‘zMU, 28-aprel, 2022, Toshkent, O‘zbekistan, I qism, 245-246 b.

14. Bozorov A.X, Raximberdiyev Q.B. Kriptografik xavfsiz psevdotasodifiy sonlar generatorlarini qurish muammollari Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati , 27-28-aprel, Toshkent-2022 y.

Avtoreferat “Muhammad al-Xorazmiy avlodlari” ilmiy jurnali tahririyatida tahrirdan o‘tkazildi va o‘zbek, rus, ingliz tillaridagi matnlarini mosligi tekshirildi

Bosishga ruxsat etildi: 27.10.2025-yil
Bichimi 60x84 $^{1}/_{16}$, «Times New Roman»
garniturada raqamli bosma usulida bosildi.
Shartli bosma tabog‘i 3,2. Adadi: 100. Buyurtma: № 95.

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