TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

XUDOYKULOV ZARIFJON TURAKULOVICH

BUYUMLAR INTERNETI TIZIMIDA AXBOROTNI KRIPTOGRAFIK HIMOYALASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc)
DISSERTATSIYASI AVTOREFERATI

Toshkent-2025

UDK: 004.056.55

Texnika fanlari doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора (DSc) по техническим наукам

Contents of dissertation abstract of the doctor (DSc) on technical sciences

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

XUDOYKULOV ZARIFJON TURAKULOVICH

BUYUMLAR INTERNETI TIZIMIDA AXBOROTNI KRIPTOGRAFIK HIMOYALASH USULLARI VA ALGORITMLARI

05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi

TEXNIKA FANLARI DOKTORI (DSc)
DISSERTATSIYASI AVTOREFERATI

Toshkent-2025

Texnika fanlari doktori (DSc) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2025.3.DSc/T982 raqam bilan ro‘yxatga olingan.

Dissertatsiya Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida bajarilgan.

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

Ilmiy maslahatchi:	**Ganiyev Salim Karimovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Kerimov Kamil Fikratovich** texnika fanlari doktori, professor
	Jurayev Gayrat Umarovich fizika-matematika fanlari doktori, professor
	Kuryazov Davlatyor Matyakubovich fizika-matematika fanlari doktori
Yetakchi tashkilot:	**Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 raqamli Ilmiy kengashning 20__-yil “__”-_____ soat ___ dagi majlisida bo‘lib o‘tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43, faks: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Dissertatsiya bilan Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (№____-raqam bilan ro‘yxatga olingan). (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-65-44).

Dissertatsiya avtoreferati 20__-yil “___”-_____da tarqatildi.
(20__-yil “__”-_____dagi №___-raqamli reestr bayonnomasi).

B.Sh. Maxkamov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, iqtisodiyot fanlari doktori, professor

M.S. Saitkamolov
Ilmiy darajalar beruvchi Ilmiy kengash ilmiy kotibi, iqtisodiyot fanlari doktori, dotsent

D.Ya. Irgasheva
Ilmiy darajalar beruvchi Ilmiy kengash qoshidagi Ilmiy seminar raisi, texnika fanlari doktori, professor

KIRISH (fan doktori (DSc) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahonda axborot kommunikatsiya infratuzilmalarida Buyumlar Interneti (Internet of Things, IoT) qurilmalarining tez o‘zlashtirilishi samaradorlikni oshirilishiga, operatsion xarajatlarni kamayishiga olib kelishi bilan bir qatorda, axborot xavfsizligi bilan bog‘liq muammolarni ham keskin oshishiga sababchi bo‘lmoqda. “IoTforAll” media platformasining ma’lumotiga ko‘ra, IoT qurilmalariga nisbatan oyiga o‘rtacha 5400 ta hujum amalga oshirilib, muvaffaqiyatli hujumning narxi 330 000 dollardan yuqori bo‘lgan, 2025-yilda kiberjinoyatlardan ko‘riladigan zarar miqdori 10 trillion dollardan yuqori bo‘lishi kutilmoqda[1]. IoT qurilmalarning axborot kommunikatsiya infratuzilmalarida boshqa tizimlar bilan aloqa o‘rnatishi mumkinligi bois, ma’lumotlarni uzatishda va saqlashda xavfsizlikni ta’minlash muhim hisoblanadi. Shu sababli, bugungi kunda IoT qurilmalari uchun mos, ma’lumotlarni uzatishda va saqlashda xavfsizlikni ta’minlovchi himoya usullari va algoritmlarini ishlab chiqishga alohida ahamiyat qaratilmoqda.

Jahonda IoT muhitida axborot xavfsizligi muammolarini tadqiqlashga, tahdidlarni oldini oluvchi ishonchli himoya mexanizmlarini ishlab chiqishga qaratilgan ilmiy-amaliy tadqiqot ishlari olib borilmoqda. Bu borada, cheklangan hisoblash va quvvat imkoniyatiga ega IoT qurilmalari uchun mo‘ljallangan, axborotning konfidensialligini, yaxlitligini, xabar manbasi autentifikatsiyasini ta’minlovchi kriptografik usul va algoritmlarni ishlab chiqish, mavjud algoritmlarni moslashtirish, kriptotahlil usullariga baholash hamda dasturiy va apparat ko‘rinishlarda amalga oshirishga qaratilgan tadqiqot ishlariga alohida e’tibor qaratilmoqda. Mazkur sohada olib borilgan ilmiy izlanishlar, tanlovlar (NIST LWC), loyihalar (CAESAR, eSTREAM) va standartlashtirish jarayonlari (ISO/IEC 29192) natijasida IoT qurilmalari uchun mo‘ljallangan xalqaro va milliy standart kriptografik algoritmlar, foydalanish uchun tavsiya etilgan kriptografik algoritmlar ishlab chiqildi, kriptotahlil usullariga baholandi va foydalanish uchun qabul qilindi.

Respublikamizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta’lim, sog‘liqni saqlash va qishloq xo‘jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish bo‘yicha kompleks chora-tadbirlarni o‘z ichiga olgan “Raqamli O‘zbekiston – 2030” strategiyasi doirasida elektron hukumatni rivojlantirish, raqamli industriyani rivojlantirish, sog‘liqni saqlash tizimini rivojlantirish, sanoat va qurilish sohalarini rivojlantirish, raqamli ta’limni rivojlantirish, raqamli infratuzilmani rivojlantirish sohasiga oid ko‘plab vazifalar amalga oshirilib kelinmoqda[2]. Mazkur vazifalar ijrosini samarali tashkil etishda, jumladan, IoT qurilmalari yordamida aqqli shahar/uy tizimlarini ishlab chiqish, inson sog‘lig‘ini doimiy nazorat qilish, sanoat sohasida jarayonlarni avtomatlashtirish masalalariga joriy etishda yuzaga keladigan axborot xavfsizligi muammolarini oldini olish, kiberhujumlarga o‘z vaqtida javob berish,

[1] https://www.iotforall.com/iot-telecom-vulnerabilities

[2] O‘zbekiston Respublikasi Prezidentining 05-oktabr 2020-yildagi PF-6079-son ““Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni.

axborotni himoyalashning ishonchli mexanizmlarini ishlab chiqish va tatbiq etish maqsadga muvofiq hisoblanadi.

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi 2022-yil 15-apreldagi O‘RQ-764-son Qonuni, O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son “2022 – 2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi Farmoni, 2024-yil 15-avgustdagi PQ-293-son “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi, 2007-yil 3-apreldagi PQ-614-son “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida” Qarorlari hamda mazkur faoliyatga tegishli boshqa me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga mazkur dissertatsiya tadqiqoti ma’lum darajada xizmat qiladi.

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

Dissertatsiya mavzusi bo‘yicha xorijiy ilmiy tadqiqotlar sharhi. IoT qurilmalari uchun mos simmetrik shifrlash, ochiq kalitli shifrlash, elektron raqamli imzo, xesh funksiya va psevdotasodifiy sonlar generatori algoritmlarini ishlab chiqish, mavjudlarini takomillashtirish va ularni zamonaviy kriptotahlil usullari yordamida baholashga yo‘naltirilgan ilmiy izlanishlar jahonning yetakli ilmiy markazlarida va oliy ta’lim muassasalarida olib borilgan va olib borilmoqda. IoT qurilmalari uchun mos algoritmlarni tanlab olish bo‘yicha Yevropa ittifoqi tomonidan o‘tkazilgan eSTREAM loyihasi, xalqaro kriptologik tadqiqotlar jamiyati tomonidan o‘tkazilgan CAESAR loyihasi, Yaponiya elektron hukumat tizimi tomonidan o‘tkazilgan CRYPTREC loyihasi, AQSHning NIST instituti tomonidan o‘tkazilgan NIST LWC tanlovi hamda ISO/IEC 29192 seriyali standartlari mazkur sohada bajarilgan ishlarga misoldir.

IoT qurilmalarida ishlovchi kriptografik algoritmlarga nisbatan “yengil vaznli (lightweight)” sifati ishlatilib, bu algoritmlar ishlashida hisoblash va quvvat resurslarini kam talab etishi bilan xarakterlanadi. Yengil vaznli simmetrik kriptografik algoritmlarni yaratishga qaratilgan ilmiy tadqiqotlar dunyoning eng ilg‘or va yetakchi ilmiy tekshirish institutlari, ilmiy-tadqiqot markazlari va oliy o‘quv yurtlarida, shu jumladan NIST instituti (AQSh), Graz Texnologiya Universiteti (Austria), Infineon Technologies (Germany), Lamarr Security Research (Austria), Radboud Universiteti (Niderlandiya), NTT (Nippon Telegraph and Telephone) (Yaponiya), Ruhr University Bochum (Germaniya), Carnegie Mellon University (AQSh), Nanyang Texnologiya Universiteti (Singapur), Janubiy Federal Universitet (Rossiya Federatsiyasi) va respublikamizda Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti, “UNICON.UZ” Fan-texnika va marketing tadqiqotlari markazi va “Kiberxavfsizlik markazi” davlat unitar korxonasida olib borilmoqda.

Yengil vaznli kriptografiya bo‘yicha dunyoda faqat AQSH hukumati o‘zining standart (Ascon) algoritmiga ega. O‘zbekiston Respublikasida ma’lumotlarni shifrlash algoritmi sifatida O‘zMSt 270:2024 standarti, xeshlash funksiya algoritmi sifatida O‘zMSt 285:2024 standarti foydalanilib kelinmoqda.

Muammoning o‘rganilganlik darajasi. Bugungi kunda yengil vaznli kriptografik algoritmlarni ishlab chiqish, ularni kriptotahlil usullariga baholash masalalari bir qator xorijiy olimlar, jumladan: A.Bogdanov, C.Dobraunig, J.Daemen, V.Rijmen, B.Guido, G.Bertoni, R.Beaulieu, A.E.Jukov, A.Luykx, N.Mouha, G.Tsudik, J.Guo, P.Duong, X.Huang, L.Yan, S.Banik, W.Zhang, D.Goudarzi, A.Canteaut, D.Bellizia, Z.Gong, C.Beierle, A.Thakor, E.Adreeva, Z.Bao, B.Bilgin, M.Hell, H.Wu va boshqalarning ilmiy ishlarida ko‘rib chiqilgan.

Axborotni himoyalashning kriptografik usullari, jumladan, kriptografik algoritmlarni ishlab chiqish, kriptotahlil usuliga baholash, apparat va dasturiy ko‘rinishlarda amalga oshirish masalalari bilan bog‘liq tadqiqotlar J.Daemen, V.Rijmen, B.Guido, G.Bertoni, B.Shnayer, K.McKay, E.K.Shannon, K.Nyberg, N.T.Courtois, J.Kelsey, K.Tsantikidou, M.Dansarie, M.Matsui, E.Ishukova, L.Babenko, P.Xasanov, M.Aripov, S.K.Ganiyev, M.M.Karimov, B.F.Abdurakhimov, D.E.Akbarov, G.U.Jurayev, A.V.Kabulov, D.M.Kuryazov, G.N.Tuychiyev, X.P.Xasanov, O.P.Axmedova, A.B.Sattorov, B.Axmedov, I.M.Boyquziyev, O.M.Allanov, R.H.Alaev, M.A.Berdimurodov kabi olimlar tomonidan tadqiq qilingan.

Shu bilan birga keng tarqalgan yengil vaznli kriptografik algoritmlardagi chiziqsiz akslantirishlarni kengaytirilgan kriptografik talablarga baholash, yon-kanal (side-channel) hujumiga bardoshli, apparat amalga oshirishga qulay yangi chiziqsiz akslantirishlarni ishlab chiqish, yengil vaznli simmetrik kriptografik algoritmlarni, psevdotasodifiy sonlar generatorini yaratish yo‘nalishlarida yetarli darajada ilmiy izlanishlar olib borilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya ishi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining ilmiy-tadqiqot ishlari rejasining 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP “Developing Services for Individuals with Disabilities–DECIDE” (2019-2022) va 10/18-F “Antivirus dasturiy vositalarini yaratish va zararli kodlarni o‘rganish bo‘yicha “Antivirusli himoya” ilmiy laboratoriyasini tashkil etish asosida tizimli qo‘llab-quvvatlash” (2018-2020) mavzusidagi loyihalar doirasida bajarilgan.

Tadqiqotning maqsadi imkoniyati cheklangan qurilmalarda axborot xavfsizligini ta’minlash (konfidensiallik, yaxlitlik va manba autentifikatsiyasi) hamda psevdotasodifiy qiymatlarni generatsiyalash imkonini beruvchi kriptografik usul va algoritmlarni takomillashtirish, ishlab chiqish va kriptotahlil usullariga baholashdan iborat.

Tadqiqotning vazifalari:

zamonaviy yengil vaznli kriptografik algoritmlarda foydalanilgan turli o‘lchamli S jadvallarni kengaytirilgan umumiy kriptografik talablarga baholash;

yengil vaznli kriptografik algoritmlarda foydalanish uchun turli o‘lchamli S jadvallarni hosil qilish usulini takomillashtirish;

yengil vaznli autentifikatsiyalangan shifrlash algoritmlarini ishlab chiqish;

yengil vaznli kalitli, kalitsiz xesh funksiyalarni qurish usuli va algoritmlarini ishlab chiqish;

yengil vaznli psevdotasodifiy sonlar generatori algoritmini ishlab chiqish;

ishlab chiqilgan yengil vaznli kriptografik algoritmlarning kriptotahlilini amalga oshirish.

Tadqiqotning obyekti sifatida imkoniyati cheklangan qurilmalarda axborotni himoyalash jarayoni olingan.

Tadqiqotning predmetini imkoniyati cheklangan qurilmalarda axborotni himoyalashning kriptografik usul va algoritmlarini tadqiqlash tashkil etadi.

Tadqiqotning usullari. Tadqiqot jarayonida axborot nazariyasi, ehtimollar nazariyasi, to‘plamlar nazariyasi, diskret matematika, sonlar nazariyasi, kriptografik algoritmlarni qurish, kriptografik algoritmlarni xavfsizlik darajalarini baholash, obyektga yo‘naltirilgan dasturlash asosida kriptografik algoritmlarni dasturiy vosita ko‘rinishida amalga oshirish usullaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

mavjud yengil vaznli kriptografik algoritmlarni xavfsizlik nuqtai nazaridan tahlil qilish maqsadida kengaytirilgan umumiy kriptografik talablarga asoslangan holda mavjud yengil vaznli kriptografik algoritmlarda qo‘llanilgan turli o‘lchamli chiziqsiz akslantirishlar baholanilgan;

xavfsizlik va apparat amalga oshirish nuqtai nazaridan yuqori ko‘rsatkichlarga ega turli o‘lchamli chiziqsiz akslantirishlarni hosil qilish maqsadida kengaytirilgan sinus va tent funksiyalaridan kombinatsion tarzda foydalanish orqali S jadvallarni generatsiyalash usuli takomillashtirilgan hamda affin akslantirishi yordamida chiziqsiz sath xususiyatlarini yaxshilash orqali S jadvallarni generatsiyalash algoritmi ishlab chiqilgan;

ma’lumotlarni konfidensialligini, yaxlitligini ta’minlashga, buyumlar interneti qurilmalarida amalga oshirishga imkon beruvchi, turli uzunlikdagi kalit va blok uzunliklarini madadlovchi yengil vaznli kriptografik algoritmlar ishlab chiqilgan;

ma’lumotlarni yaxlitligini, manba autentifikatsiyasini ta’minlashga, buyumlar interneti qurilmalarida amalga oshirishga imkon beruvchi, o‘zgaruvchan hamda o‘zgarmas uzunlikdagi xesh qiymatlarni hosil qilishni madadlovchi yengil vaznli kriptografik usul va algoritmlar ishlab chiqilgan;

yagona kiritilgan qiymatlardan yetarli uzunlikdagi psevdotasodifiy ketma-ketliklarni hosil qilishga, buyumlar interneti qurilmalarida amalga oshirishga, mukammal xavfsizlikni ta’minlashga imkon beruvchi yengil vaznli kriptografik algoritm ishlab chiqilgan;

qurilish arxitekturasi va raund akslantirishlarining kriptobardoshlik darajasini aniqlashga imkon beruvchi umumiy kriptotahlil usullar, chiziqli, algebraik va integral kriptotahlil usullari yordamida ishlab chiqilgan yengil vaznli kriptografik algoritmlar baholanilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

keng tarqalgan yengil vaznli kriptografik algoritmlardagi turli o‘lchamli chiziqsiz akslantirishlarni kengaytirilgan kriptografik talablar asosida baholovchi dasturiy vosita ishlab chiqilgan;

kengaytirilgan sinus va tent xaotik akslantirishlaridan kombinatsion tarzda foydalanishga asoslangan turli o‘lchamli S jadvallarni hosil qiluvchi dasturiy vosita ishlab chiqilgan;

affin akslantirishini kriptografik algoritmning chiziqsiz sathi xususiyatlariga ta’sirini o‘rganish asosida yon-kanal hujumlariga bardoshli, apparat amalga oshirishga qulay S jadvallarni hosil qiluvchi dasturiy vosita ishlab chiqilgan;

turli holat uzunlikli raund akslantirishlariga ega sponge konstruksiyasi asosida ma’lumotlarni autentifikatsiyalangan shifrlash imkoniyatli kriptografik algoritmlarning dasturiy vositalari ishlab chiqilgan;

turli holat uzunlikli raund akslantirishlariga ega sponge konstruksiyasi asosida ma’lumotlarni kalitli va kalitsiz xeshlab, o‘zgaruvchan hamda o‘zgarmas uzunlikdagi xesh qiymatlarni hosil qiluvchi kriptografik algoritmlarning dasturiy vositalari ishlab chiqilgan;

sponge konstruksiyasi asosida mukammal xavfsizlikni ta’minlovchi psevdotasodifiy sonlarni hosil qilish algoritmining dasturiy vositasi ishlab chiqilgan;

ishlab chiqilgan yengil vaznli kriptografik algoritmlar qurilish xususiyatiga ko‘ra umumiy kriptotahlil usullariga, raund akslantirishlari xususiyatiga ko‘ra chiziqli, algebraik va integral kriptotahlil usullariga baholash orqali kriptografik bardoshliklari isbot qilingan.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi taklif etilgan algoritmlarga nisbatan qat’iy matematik tadqiqotlar o‘tkazilib, hisoblash tajribalari natijalarini umumqabul qilingan mezonlar asosida taqqoslash orqali isbotlangan va sonli tadqiqotlar natijalari bilan tasdiqlangan. Kengaytirilgan kriptografik talablarga baholash, S jadvallarni hosil qilish algoritmlarini to‘g‘ri ishlashi, taklif etilgan shifrlash, xeshlash va psevdotasodify sonlar generatori algoritmlarini tezliklari va xotira hajmlari haqidagi ma’lumotlar ishlab chiqilgan tegishli dasturiy vositalar bilan tekshirilgan.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati sifatida chiziqsiz akslantirishlarni hosil qilish usuli, shuningdek, sponge konstruksiyasi uchun raund akslantirishlarini hosil qilish usuli va u asosida ishlab chiqilgan yengil vaznli kriptografik algoritmlar xizmat qiladi.

Tadqiqotdan olingan natijalarning amaliy ahamiyati esa, chiziqsiz akslantirishlarni baholash uchun tanlab olingan kengaytirilgan kriptografik talablardan Respublikada amalga oshiriladigan tanlovlarda algoritmlarni tanlab olishdagi tegishli uslub sifatida, bardoshligi yuqori, tezkor va turli holat uzunliklariga ega raund akslantirishlaridan esa yangi yengil vaznli kriptografik algoritmlarni qurishda foydalanilishi mumkinligi bilan begilanadi.

Tadqiqot natijalarining joriy qilinishi. Buyumlar Interneti tizimida axborotni kriptografik himoyalash usullari va algoritmlari mavzusidagi tadqiqot ishida olingan ilmiy natijalar asosida:

mavjud yengil vaznli kriptografik algoritmlarni xavfsizlik nuqtai nazaridan tahlil qilish maqsadida kengaytirilgan umumiy kriptografik talablarga asoslangan holda baholanilgan chiziqsiz akslantirishlarni o‘z ichiga olgan yengil vaznli kriptografik algoritmlarning dasturiy vositalari “O‘zbektelekom” AK Jabuniy-G‘arbiy filiali ishchi muhitida axborotni kriptografik himoyalash maqsadida tadbiq etilgan (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida ma’lumotni konfidensialligini va yaxlitligini ta’minlovchi AEAD_P320 algoritmi qolganlariga nisbatan eng yuqori (o‘rtacha 345.62 MB/s) tezlikni, AEAD_P384 algoritmiga nisbatan 1.02 marta yuqori tezlikni qayd etgan.

xavfsizlik va apparat amalga oshirish nuqtai nazaridan yuqori ko‘rsatkichlarga ega turli o‘lchamli chiziqsiz akslantirishlarni hosil qilish maqsadida kengaytirilgan sinus va tent funksiyalaridan kombinatsion tarzda foydalanish orqali takomillashtirilgan usul yordamida hosil qilingan S jadvallarni o‘z ichiga olgan yengil vaznli kriptografik algoritmlarning dasturiy vositalari “Kiberxavfsizlik markazi” DUK test laboratoriyasida ma’lumotlarni himoyalash maqsadida joriy etilgan (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida psevdotasodifiy sonlar generatorining dasturiy vositasi kriptografik algoritmlar uchun talab etilgan psevdotasodifiy qiymatlarni o‘rtacha 53.932 MB/s tezlik bilan generatsiyalash imkonini bergan.

ma’lumotlarni konfidensialligini, yaxlitligini ta’minlashga, buyumlar interneti qurilmalarida amalga oshirishga imkon beruvchi, turli uzunlikdagi kalit va blok uzunliklarini madadlovchi yengil vaznli kriptografik algoritmlarga asoslangan dasturiy vositalar “O‘zkomnazorat” inspeksiyasi Samarqand viloyati hududiy shu’basi faoliyatida resurslari cheklangan qurilmalarda axborotni himoyalash maqsadida tadbiq etilgan (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida ma’lumotlarni konfidensialligini, yaxlitligini ta’minlovchi AEAD_P320 algoritmi o‘rtacha 17.31 Kbayt ROM va 0.90 Kbayt RAM xotira hajmini talab etib, 32 bitli mikrokontrollerlarda ham samarali amalga oshirish mumkinligini ko‘rsatgan, bunda barcha algoritmlar mikrokontrollerning ko‘pi bilan 3% ROM va 2% RAM xotira qismini band qilish imkonini bergan.

ma’lumotlarni yaxlitligini, manba autentifikatsiyasini ta’minlashga, buyumlar interneti qurilmalarida amalga oshirishga imkon beruvchi, o‘zgaruvchan hamda o‘zgarmas uzunlikdagi xesh qiymatlarni hosil qilishni madadlovchi yengil vaznli kriptografik xesh funksiya algoritmi asosida ishlab chiqilgan dasturiy vositalar “UNICON.UZ” - Fan-texnika va marketing tadqiqotlari markazi” mas’uliyati cheklangan jamiyatining sinov laboratoriyasida Arduino Mega platasida turli uzunlikdagi ma’lumotlarni xeshlash uchun tadbiq etilgan (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida barcha algoritmlar 512 baytli ma’lumotni xeshlash uchun mikrokontrollerning 3% gacha ROM, 5% gacha RAM xotirasini talab etib, buning uchun 0.2 sekund vaqt, 20.5 mJ energiya sarflanishiga imkon bergan.

yagona kiritilgan qiymatlardan yetarli uzunlikdagi psevdotasodifiy ketma-ketliklarni hosil qilishga, buyumlar interneti qurilmalarida amalga oshirishga, mukammal xavfsizlikni ta’minlashga imkon beruvchi yengil vaznli kriptografik algoritm asosida ishlab chiqilgan dasturiy vosita “Intsoft-servis” MChJda Arduino Leonardo platasida turli uzunlikdagi psevdotasodifiy qiymatlarni generatsiyalash maqsadida joriy etilgan (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida psevdotasodifiy sonlarni generatsiyalash algoritmi 8 bitli mikrokontrollerda 34% ROM xotira hajmi va 21% RAM xotira hajmiga ega bo‘lib, 0.04 sekund vaqt va 2.42 mJ energiya energiya sarfi bilan 256 baytli qiymatni hosil qilishga imkon bergan.

qurilish arxitekturasi va raund akslantirishlarining kriptobardoshlik darajasini aniqlashga imkon beruvchi umumiy kriptotahlil usullar, chiziqli, algebraik va integral kriptotahlil usullari yordamida baholangan yengil vaznli kriptografik algoritmlar asosida ishlab chiqilgan dasturiy vositalar “UNICON.UZ” - Fan-texnika va marketing tadqiqotlari markazi” mas’uliyati cheklangan jamiyatining sinov laboratoriyasida joriy etildi (Raqamli texnologiyalar vazirligining 2025-yil 17-sentabrdagi 33-8/6636-sonli ma’lumotnomasi). Ilmiy tadqiqot natijasida taklif etilgan algoritmlar chiziqli, algebraik va integral kriptotahlil usullariga bardoshlikni ta’minlab, 8 bitli mikrokontrollerlarda ham kichik xotira hajmini talab etgan holda, amalga oshirishga imkon bergan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 3 ta xalqaro va 8 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiyaning mavzusi bo‘yicha jami 30 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida 15 ta maqola, shulardan, 6 tasi xorijiy va 9 tasi respublika jurnallarida nashr etilgan hamda EHM uchun yaratilgan 4 ta dasturiy vositalarni qaydlash guvohnomalari olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, beshta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiya hajmi 174 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zarurati keltirilib, tadqiqotning O‘zbekiston Respublikasi 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 ochib berilgan, tadqiqot natijalarini amalga tatbiq etish ro‘yxati taqdim qilingan, nashr etilgan ishlar va dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning **“Buyumlar interneti tizimida axborotni kriptografik himoyalashdagi muammolar”** deb nomlanuvchi birinchi bobi buyumlar interneti tizimlarida foydalaniluvchi kriptografik algoritmlarning xususiyatlari, yengil vaznli kriptografik algoritmlarning tahlil natijalari, keng tarqalgan yengil vaznli

kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlarni kengaytirilgan umumiy kriptografik talablarga baholash natijalari bayon qilingan.

IoT ssenariysida xavfsizlik muhim ahamiyatga ega. Bunda xavfsizlik masalalari turli darajalarda, texnologik muammolardan tortib, undan yuqori masalalar, masalan, smart o‘yinchoqlarda shaxsiylik va ishonchlikni ta’minlash uchun qo‘llaniladi. Xavfsizlik muammolari smart obyektlarning tabiati va standart protokollaridan kelib chiqadi. IoT muhitini tashkil etish uchun turli arxitekturalar taklif etilgan bo‘lib, ular orasida 1) ilova va xizmat vazifalari amalga oshiriluvchi ilova sathi (Application layer), 2) tarmoq/ uzatish sathi (Network/ Transmission layer) va 3) chetki nuqtalar (sensorlar)ga aloqador bo‘lgan ma’lumotlarni to‘plash/ chetki sathlaridan (Perception/ Edge layer) iborat bo‘lgan 3 qatlamli sath muhim ahamiyat kasb etadi. Mazkur arxitekturaning chetki va tarmoq sathlarida axborotning konfidensialligini, yaxlitligini, manba autentifikatsiyasini ta’minlashda va psevdotasodifiy sonlarni hosil qilishda kriptografik algoritmlar muhim ahamiyat kasb etadi.

IoT qurilmalari odatda cheklangan quvvat manbalari va kichik hisoblash imkoniyatiga ega bo‘lgani bois, mazkur manbalardan samarali foydalanish muhim hisoblanadi (1-jadval). Xususan, xavfsizlik vositalaridan, kriptografik himoya vositalaridan foydalanganda ham bunga etibor berish kerak bo‘ladi. Olib borilgan tadqiqotlar natijalari esa mavjud ananaviy kriptografik algoritmlarni IoT qurilmalari uchun o‘rinli emasligini ko‘rsatmoqda. Bu esa cheklangan quvvat manbalari va kichik hisoblash imkoniyatiga ega qurilmalar uchun mos kriptografik algoritmlarni ishlab chiqish zaruriyatini keltirib chiqaradi.

1-jadval

RFC7228 bo‘yicha imkoniyati cheklangan qurilmalarning sinflari (KiB = 1024 bayt, Random Access Memory – RAM, Read Only Memory - ROM)

Nomi	Ma’lumot hajmi (RAM)	Kod o‘lchami (ROM, Flesh xotira)
Sinf 0, C0	≪10 KiB	≪100 KiB
Sinf 1, C1	~10 KiB	~100 KiB
Sinf 2, C2	~50 KiB	~250 KiB

Mazkur qurilmalar uchun mo‘ljallangan kriptografik algoritmlarga nisbatan “yengil vaznli (lightweight)” sifati ishlatilib, bu algoritmning xavfsizlik darajasini saqlab qolgan holda, amalga oshirishda kam quvvat sarfini va kichik hisoblash imkoniyatini talab etishi bilan xarakterlanadi.

IoT qurilmalari uchun hozirgacha ko‘plab kriptografik algoritmlar ishlab chiqilgan bo‘lib, ularning ba’zilari o‘tkazilgan tanlovlar natijasida davlatlarning milliy standarti yoki xalqaro miqiyosidagi standart sifatida qabul qilingan. Bularga 2004-2008-yillarda apparat va dasturiy amalga oshirishga mo‘ljallangan oqimli shifrlarni tanlab olish uchun tashkil etilgan eSTREAM loyihasini, turli muhitlarda foydalanish uchun aloqador ma’lumot bilan autentifikatsiyalovchi shifrlash (Authenticated Encryption with Associated Data, AEAD) turidagi algoritmlarni tanlab olish uchun 2012-2019-yillar oralig‘ida xalqaro kriptologik tadqiqotlar jamiyati tomonidan o‘tkazilgan CAESAR loyihasini, NIST tomonidan 2015-2023-yillar oralig‘ida o‘tkazilgan NIST LWC tanlovini, Yaponiya elektron hukumat tizimlarida foydalanilgan kriptografik mexanizmlarning xavfsizligini

baholash va monitoringni amalga oshirish maqsadida tashkil etilgan CRYPTREC loyihasini hamda ISO/IEC (International Organization of Standardization/ International Electrotechnical Commission) 29192 (Information technology - Security techniques - Lightweight cryptography) seriyali standartini misol keltirish mumkin.

Yuqorida keltirilgan tanlovlarda, loyihalarda va standartlarda keltirilgan yengil vaznli kriptografik algoritmlar shifrlash, AEAD turidagi shifrlash, xabarlarni autentifikatsiyalash kodlari (Message Authentication Code, MAC), xesh funksiyalar kabi algoritmlar guruhlariga ajratilgan holda qurilish asosi, parametrlari, apparat-dasturiy amalga oshirish natijalari, kriptotahlil usullariga baholash natijalari kabi xususiyatlari bo‘yicha tahlil qilindi. Xususan, 2-jadvalda yengil vaznli AEAD shifrlash algoritmlari va ularning xususiyatlari keltirilgan. Tahlil natijalari mavjud yengil vaznli kriptografik algoritmlarni apparat-dasturiy amalga oshirish va kriptotahlil usullariga, xususan yon-kanal (side-channel) hujumlariga bardoshligi bilan bog‘liq kamchiliklarga ega ekanligini ko‘rsatdi.

Barcha simmetrik kriptografik algoritmlarda bardoshlikni ta’minlashda chiziqsiz akslantirishlar muhim ahamiyat kasb etadi. Shu sababli chiziqli akslantirishlarni foydalanishdan oldin umumiy kriptografik talablarga baholash, uni kriptotahlil usullariga bardoshli bo‘lishini ta’minlaydi.

2-jadval

Yengil vaznli AEAD shifrlash algoritmlari

Nomi	Turi	Asos akslantirish	Holati (bit)	Kalit (bit)	Rate/ blok uzunligi (bit)	Teg (bit)	Xavfsizlik (bit)
Ascon	Sponge	**Ascop-p**	**320**	**128**	**64**	**128**	**128**
		Ascon-p	320	128	128	128	128
Elephant	Sponge	**Spongent**	**160**	**128**	**160**	**64**	**112**
		Spongent	176	128	176	64	127
		Keccak	200	128	176	128	127
GIFT-COFB	Blokli	**GIFT-128**	**192**	**128**	**128**	**128**	**128**
Grain-128AEAD	Oqimli	**Grain-128a**	**256**	**128**	**1**	**64**	**128**
ISAP	Sponge	Keccak	400	128	144	128	128
		Ascop-p	**320**	**128**	**64**	**128**	**128**
		Keccak	400	128	144	128	128
		Ascop-p	320	128	64	128	128
PHOTON-Beetle	Sponge	**PHOTON256**	**256**	**128**	**128**	**256**	**121**
		PHOTON256	256	128	32	256	128
Romulus	Blokli	**Skinny-128-384**	**384**	**128**	**128**	**128**	**128**
		Skinny-128-384	384	128	128	128	128
		Skinny-128-384	384	128	128	128	128
SPARKLE	Sponge	**SPARKLE**	**256**	**128**	**128**	**128**	**120**
		SPARKLE	384	128	256	128	120
		SPARKLE	384	192	192	192	184
		SPARKLE	512	256	256	256	248
TinyJambu	Sponge	**TinyJambu**	**128**	**128**	**32**	**64**	**120**
Xoodyak	Sponge	**Xoodoo**	**384**	**128**	**352**	**128**	**128**
AES-GCM	Blokli	**AES**	**128**	**128, 256**	**128**	96, 104, 112,120, **128**	64 **128**

Izoh: Parametrlari qalin qora rangda berilganlari mualliflar tomonidan taqdim etilgan asosiy variantlar.

Umumiy kriptografik talablar asosan ananaviy chiziqsiz akslantirishlarni baholashga mo‘ljallangan bo‘lib, yengil vaznli kriptografik algoritmlardagi

chiziqsiz akslantirishlarni baholashda qo‘shimcha kriteriylarni kiritish zarur hisoblanadi. Shu sababli yengil vaznli kriptografik algoritmlardagi chiziqsiz akslantirishlarni baholashda quyidagi kriteriylardan iborat bo‘lgan kengaytirilgan umumiy kriptografik talablardan foydalanildi:

- umumiy kriteriylar: muvozanatlashganlik va muntazamlik, qat’iy lavin samaradorlik darajasi (Strict Avalanche Criterion, SAC), bitlar bog‘liqsizligi mezonini (Bit Independence Criterion, BIC), o‘zgarmas (Fixed point, FP) va teskari o‘zgarmas nuqtalar (Opposed fixed point, OFP);
- chiziqli kriptotahlilga bardoshlikni ko‘rsatuvchi kriteriylar: chiziqsizlik (Nonlinearity, NL), korrelyatsion immunitetga (Correlation immunity, CI), chiziqli yaqinlashish ehtimoli (Linear Approximation Probability, LP), chiziqli tarmoqlanishlar soni (Linear branch number, LBN);
- differensial kriptotahlilga bardoshlikni ko‘rsatuvchi kriteriylar: tarqalish mezoni (Propagation Criteria, PC), differensial yaqinlashish ehtimoli (Differential Approximation Probability, DP), differensial tarmoqlanishlar soni (Differential branch number, DBN);
- algebraik kriptotahlilga bardoshlikni ko‘rsatuvchi kriteriylar: algebraik immunitetlik (Algebraic immunity, AI) darajasi va talab etiluvchi tenglamalar soni (TS);
- differensial quvvat tahlili (Differential power analysis, DPA) hujumiga bardoshlikni ko‘rsatuvchi kriteriylar: shaffoflik chegarasi (Transparency order, TO), signal shovqin nisbati (Signal-to-Noise Ratio, SNR), chalkashish koeffitsiyenti dispersiyasi (Confusion coefficient variance, CCV);
- apparat amalga oshirishdagi samaradorlikni ko‘rsatuvchi kriteriy: mantiqiy elementlar (ME) soni.

Tanlab olingan kriteriylar asosida turli o‘lchamdagi S jadvallarni baholash natijalari 3-jadvalda keltirilgan.

Olingan tahlil natijalari yengil vanzli kriptografik simmetrik algoritmlarda chiziqsiz akslantirish sifatida kichik o‘lchamli S jadvallardan foydalanilganini, ularning qator kriptotahlil hujumlariga, xususan, yon-kanal hujumlariga nisbatan bardoshligi yuqori emasligini, apparat amalga oshirishda yuqori samaradorlikni qayt etmasligini ko‘rsatadi.

Dissertatsiyaning **“Yengil vaznli simmetrik kriptotizimlar uchun kriptobardoshli akslantirishlar”** deb nomlanuvchi ikkinchi bobida yengil vaznli kriptografik algoritmlarni qurishda sponge konstruksiyasining ahamiyati haqidagi ma’lumotlar, yengil vaznli kriptografik algoritmlar uchun turli uzunlikdagi chiziqsiz akslantirishlarni qurish usuli va algoritmi, turli holat uzunliklari uchun raund akslantirishini qurish tartibi hamda ulardan olingan natijalar tahlili keltirilgan.

Xususan, 2.1-paragrafda yengil vaznli kriptografik algoritmlarni qurishda sponge konstruksiyasining ahamiyati asoslangan. Yengil vaznli kriptografik algoritmlarni qurishda asosan sponge (shimgich) konstruksiyasidan keng foydalanilganini 2-jadvaldan ko‘rish mumkin. *Sponge konstruktsiyasi* – bu o‘zgaruvchan uzunlikdagi kiruvchi xabardan istalgan uzunlikdagi chiqishni hosil qilish uchun ishlatiladigan oddiy iterativ (bosqichli) konstruksiya bo‘lib, u o‘zgarmas uzunlikdagi b bitlar ustida ishlaydigan akslantirish (transformation) yoki

o‘rin almashtirish (permutation) funksiyasi f ga asoslanadi. Bu yerda, b – umumiy holat (state) hajmi deb ataladi (1-rasm). Sponge konstruktsiyasi $b = r + c$ bitli holatda ishlaydi, bu yerda: r - (kiritiladigan/ chiqariladigan) ma’lumot miqdori (bitrate), c - sig‘im (capacity), xavfsizlikni ta’minlaydigan yashirin qism.

3-jadval

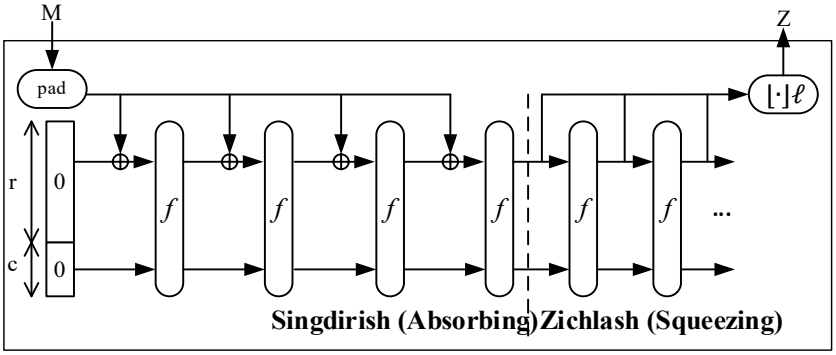
Turli o‘lchamli S jadvallarning kengaytirilgan umumiy kriptografik talablar bo‘yicha baholash natijalari

№	Manba	Umumiy					Chiziqli				Differensiyal			Alg	DPA			Ama
		B +	FP ↓	OFP ↓	SAC (=0.5)	BIC-SAC (=0.5)	NL ↑	LP ↓	CI ↑	LBN ↑	DP ↓	PC ↑	DBN ↑	AI, TS ↑	TO ↓	CCV ↑	SNR ↓	ME ↓
4x4 S jadvallar																		
1.	Present	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
2.	FEATHER	+	1	0	0.562	0.531	4	0.25	0,0,0,0	2	0.375	0	2	2, 21	3.533	0.457	2.398	23
3.	ARSHAD (8)	+	0	4	0.500	0.520	4	0.25	0,0,0,0	2	0.375	0	2	2, 21	3.666	0.382	2.259	20
4.	IVLBC	+	4	0	0.546	0.531	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.666	0.257	2.806	8
5.	DBST (1)	+	1	0	0.640	0.468	4	0.25	0,0,1,1	2	0.250	0	2	2, 21	3.600	0.307	2.685	14
6.	ELEPHANT	+	0	1	0.656	0.520	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.266	0.457	2.398	15
7.	GIFT	+	0	1	0.625	0.541	4	0.25	0,0,1,1	2	0.375	0	2	2, 21	3.600	0.457	2.398	15
8.	KNOT	+	0	2	0.671	0.479	4	0.25	1,1,0,0	2	0.250	0	2	2, 21	3.333	0.607	2.187	16
9.	PYJAMASK	+	0	2	0.593	0.520	4	0.25	1,0,0,0	2	0.250	0	2	2, 21	3.466	0.607	2.187	16
10.	SATURNIN	+	1	0	0.531	0.500	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.533	0.357	2.578	16
11.	SPOOK	+	1	2	0.515	0.562	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.666	0.307	2.685	8
12.	KLEIN	+	0	0	0.593	0.500	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.466	1.207	1.691	23
13.	RECTANGLE	+	0	0	0.671	0.479	4	0.25	0,0,1,1	2	0.250	0	2	2, 21	3.400	0.607	2.187	17
14.	PRIDE	+	4	0	0.500	0.541	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.533	0.307	2.685	8
15.	CRAFT	+	4	2	0.406	0.562	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.466	1.257	1.663	18
16.	Duong	+	0	0	0.500	0.500	4	0.25	0,0,1,0	2	0.250	0	2	2, 21	3.400	1.357	1.612	19
17.	Photon	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
18.	Magma 0	+	1	0	0.515	0.520	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.533	0.357	2.578	21
5x5 S jadvallar																		
19.	Ascon	+	0	0	0.619	0.520	8	0.25	1,1,1,1,1	3	0.250	0	3	2, 25	4.322	0.501	3.015	20
20.	PRIMATE	+	0	2	0.540	0.510	12	0.125	0,0,0,0,0	2	0.062	0	2	2, 25	4.837	0.308	3.535	27
21.	ICEPOLE	+	0	2	0.425	0.550	8	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.516	0.190	4.025	30
22.	SYCON	+	0	0	0.620	0.520	8	0.25	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	20
23.	Duong	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 25	4.580	1.275	2.085	41
24.	Thakor	+	0	1	0.540	0.507	8.4	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.596	0.347	3.408	42
25.	Irfan	+	0	0	0.540	0.525	8.8	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.532	0.259	3.713	40
6x6 S jadvallar																		
26.	Yan	+	0	2	0.503	0.754	24	0.125	1,1,1,0,0,0	2	0.062	0	2	2, 28	5.452	0.402	4.086	49
27.	Kim	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.670	0.339	4.341	44
28.	Sarkar 1	+	4	2	0.569	0.775	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 28	5.714	0.402	4.086	39
29.	Sarkar 2	+	2	0	0.565	0.764	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 28	5.595	0.342	4.328	72
30.	Bilgin	+	0	1	0.508	0.764	24	0.125	0,0,0,0,0,0	2	0.031	0	2	2, 22	5.730	0.238	4.879	73
8x8 S jadvallar																		
31.	Abdurazzokov	+	0	1	0.494	0.497	105.0	0.132	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.801	0.118	9.408	-
32.	AES	+	0	0	0.504	0.504	112.0	0.062	0,0,0,0,0,0,0,0	2	0.015	0	2	2, 39	7.860	0.111	9.599	-
33.	Kuznechik	+	0	0	0.512	0.494	106.5	0.109	0,0,0,0,0,0,0,0	2	0.031	0	2	3, 441	7.835	0.112	9.570	-
34.	Romulus	+	1	0	0.316	0.431	64.0	0.250	0,0,0,0,0,0,0,0	2	0.250	0	2	2, 34	7.174	0.340	6.312	-
35.	Manzoor	+	2	1	0.503	0.504	110	0.132	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.818	0.098	9.976	-
36.	Alqahtani	+	1	2	0.505	0.502	102.7	0.132	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.808	0.124	9.251	-

Sponge konstruktsiyasi ikkita bosqichda ishlaydi:

1. Singdirish (Absorbing) bosqichi: kiruvchi xabar r bitli bloklarga bo‘linadi va maxsus to‘ldirish (padding) usuli bilan blok uzunligiga karrali bo‘lgunga qadar to‘ldiriladi. Har bir blok holatning dastlabki r bitiga XOR amalida qo‘shiladi.

So‘ngra kiruvchi sifatida qabul qilingan holat qiymati uchun f funksiyasi qo‘llaniladi. Barcha bloklar kiritilgach, zichlash (squeezing) bosqichiga o‘tiladi.



1-rasm. Sponge konstruksiyasi

2. Zichlash (Squeezing) bosqichi: holatning dastlabki r biti chiqarish bloklari sifatida olinadi. Har bir chiqarishdan so‘ng f funksiya yana qo‘llaniladi. Foydalanuvchi istalgan uzunlikdagi chiqishni olishi mumkin. Holatning oxirgi c bitlariga hech qachon kirish bloklari tomonidan bevosita ta’sir qilinmaydi va zichlash bosqichida hech qachon chiqarilmaydi.

Ma’lumotlarni to‘ldirish qoidasi. Sponge konstruksiyasi uchun ma’lumotlarni to‘ldirishning ikki usulidan: sodda (simple) va ko‘p miqdorli (multi-rate), foydalaniladi. *Sodda to‘ldirish*, $pad10^*$ kabi belgilanib, bitta 1 bit qo‘shiladi, so‘ngra natijaning uzunligi blok uzunligining ko‘paytmasiga teng bo‘lishi uchun kerakli eng kam sondagi 0 bitlar qo‘shiladi. *Ko‘p miqdorli to‘ldirish*, $pad10^*1$ kabi belgilanib, bitta 1 bit qo‘shiladi, so‘ngra natijaning uzunligi blok uzunligining ko‘paytmasiga teng bo‘lishi uchun kerakli eng kam sondagi 0 bitlari qo‘shiladi, undan keyin yana bitta 1 bit qo‘shiladi.

Sponge konstruksiyasi *umumiy hujumlarga* nisbatan $c/2$ xavfsizlik darajasini ta’minlaydi. Xususan, kolliziyalar, ikkilamchi asl obrazni aniqlash, farqlash, soxtalashtirish va uzunlikni kengaytirish hujumiga bardoshlik $2^{c/2}$ ga; asl obrazni aniqlash $\min(2^n, 2^c)$ ga; va kalitni tiklash $\min(2^{c/2}, 2^c, 2^k)$ va o‘rtada uchrashish kalitli rejimlar uchun $\min(2^{c/2}, 2^{k/2})$ yoki kalitsiz rejimlarda asl obrazni aniqlash uchun $\min(2^n, 2^{c/2})$ xavfsizlik darajasi ta’minlanadi.

Asosiy hujumlar esa farqlashdagi imkoniyatga bog‘liq bo‘lib, agar raund akslantirishi zaif bo‘lsa $2^{c/2}$ chegara buziladi. Kalit uzunligi (k) kalitni tiklashga ta’sir qilib, kolliziyalar, soxtalashtirish yoki farqlash hujumlariga ta’sir qilmaydi (shu sababli bu yerda 2^k mos kelmaydi, agar kalitni tiklash oldinroq amalga oshirilmasa). Germetik sponge konstruksiyasi f akslantirishni yuqori diffuziyali, chiziqsizlik va farqlovchilarsiz loyihalash imkonini beradi va xavfsizlikning umumiy chegaralarga mos kelishini ta’minlaydi.

Mazkur bobning 2.2-paragrafida sponge konstruksiyasidagi raund akslantirishi uchun chiziqsiz akslantirishlarni qurish masalasi ko‘rib o‘tilgan. Dastlab xaotik akslan-tirishlarga asoslangan S jadvallarni qurishning usuli takomillashtirilgan va algoritmi taklif etilgan.

Xaotik tizimlarda kirish qiymati va chiqish qiymati o‘rtasida bevosita aloqadorlik bo‘lmaganligi bois u chiziqsiz dinamik tizimlar deb ham ataladi. Amalda

akslantirish va tizimlarni xaotiklik darajasini aniqlash uchun qator usullardan foydalanib, ular orasida bifurkatsiya diagrammasi (Bifurcation Diagram) va Lyapunov ko‘rsatkichidan (Lyapunov Exponent, LE) keng qo‘llaniladi. Masalan, logistik akslantirish (Logistic map) deb ataluvchi xaotik akslantirish quyidagicha ifodalanadi:

$$x_{n+1} = ax_n(1 - x_n),$$

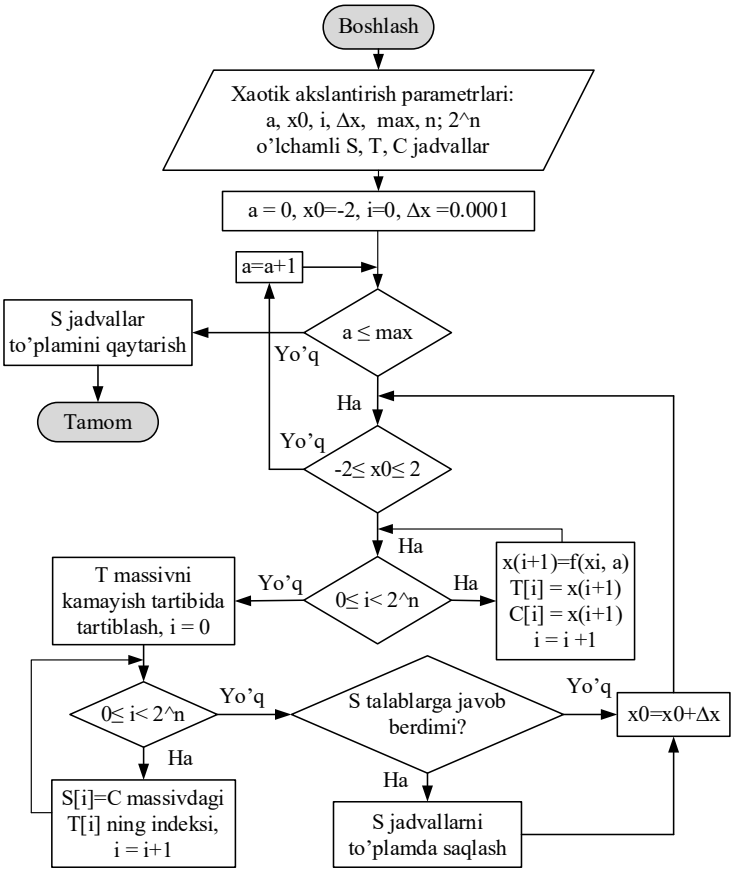
bu yerda, a – nazorat parametri, x_n –n-marta hosil qilingan qiymat.

Mazkur ishda xaotik akslantirishga asoslangan usul kengaytirilgan sinus (Enhanced Sine map) va tent (Enhanced Tent map) funksiyalaridan foydalanish orqali takomillashtirilgan:

$$x_{i+1} = f(x_i, a) = \begin{cases} \sin(a\pi\sin(\pi x_i)) + \sin(\pi a x_i) & x_i < 0.5 \\ \sin(a\pi\sin(\pi x_i)) + \sin(\pi a(1 - x_i)) & x_i \geq 0.5 \end{cases}$$

bu yerda, a nazorat parametri va $a \in (0, +\infty)$ o‘rinli. Ushbu tenglikda x_i kattaligi qiymatlari $[-2,\ 2]$ oraliqda yotadi.

Taklif etilayotgan xaotik akslantirishga asosan S jadvalni qurish algoritmi 2-rasmda keltirilgan. Ushbu algoritm xaotik akslantirishdan hosil bo‘lgan qiymatlardan S jadvalni qurishda oldindan belgilangan talablarga nisbatan tekshirishga asoslanadi. Generatsiya qilingan S jadvallarni yuqorida keltirilgan kengaytirilgan umumiy talablar bo‘yicha baholash natijalari 4-jadvalda keltirilgan.



2-rasm. S jadvalni qurish algoritmi

Bundan tashqari, affin akslantirishini S jadval xususiyatlariga ta’siri o‘rganilgan holda, yangi samarali S jadvallarni generatsiyalash algoritmi taklif etilgan.

Affin akslantirishi kriptografiyada, xususan, simmetrik blokli shifrlar va S jadvallarni loyihalashda foydalaniluvchi matematik amal o‘zida chiziqli akslantirish va o‘zgarmasga modul bo‘yicha qo‘shishni mujassamlashtirgan. Affin akslantirishi kriptografik algoritmlarda chiziqsizlik va aralashtirishni taqdim etishda yordam beradi.

4-jadval

Generatsiya qilingan S jadvallarning kengaytirilgan umumiy kriptografik talablar bo‘yicha baholash natijalari

S jadval	Umumiy					Chiziqli				Differensiyal			Alg	DPA			Ama
	B+	FP↓	OFP↓	SAC (=0.5)	BIC-SAC (=0.5)	NL↑	LP↓	CI↑	LBN↑	DP↓	PC↑	D B N ↑	AI, TS↑	TO↓	CCV↑	SNR↓	ME↓
4x4 S jadvallar																	
S_Box1	+	0	0	0.500	0.500	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.733	1.207	1.691	19
S_Box2	+	0	0	0.500	0.500	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.533	1.182	1.705	19
S_Box3	+	0	0	0.500	0.500	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.533	1.382	1.600	22
S_Box4	+	0	0	0.500	0.500	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.666	1.207	1.691	21
5x5 S jadvallar																	
S_Box1	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 24	4.645	1.194	2.144	43
S_Box2	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 24	4.661	1.293	2.072	42
S_Box3	+	0	0	0.575	0.532	9.6	0.25	0,0,0,0,0	2	0.25	0	3	2, 24	4.645	0.347	3.408	41
6x6 S jadvallar																	
S_Box1	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.599	0.339	4.341	44
8x8 S jadvallar																	
S_Box1	+	0	0	0.494	0.507	106.5	0.125	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.799	0.126	9.208	-
S_Box2	+	0	0	0.501	0.502	107	0.148	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.808	0.119	9.384	-

1-ta’rif. $GF(2^n)$ chekli maydonda affin akslantirishi quyidagicha ifodalanadi:

$$Y = A \cdot X \oplus B$$

bu yerda, X – kattalik n bitli kirish vektorini, A – esa $GF(2)$ maydonda teskarisiga ega $n \times n$ matritsa, B – kattalik n bitli o‘zgarmas vektor, Y – kattalik n bitli chiqish vektori, $\oplus$ - bitlararo XOR amalini anglatadi.

Umumiy holda mavjud S jadvaldan affin akslantirishi yordamida yangi, mavjudidan kengaytirilgan kriptografik talablar bo‘yicha yaxshi hisoblangan S jadvalni hosil qilish algoritmining blok-sxemasi 3-rasmda keltirilgan.

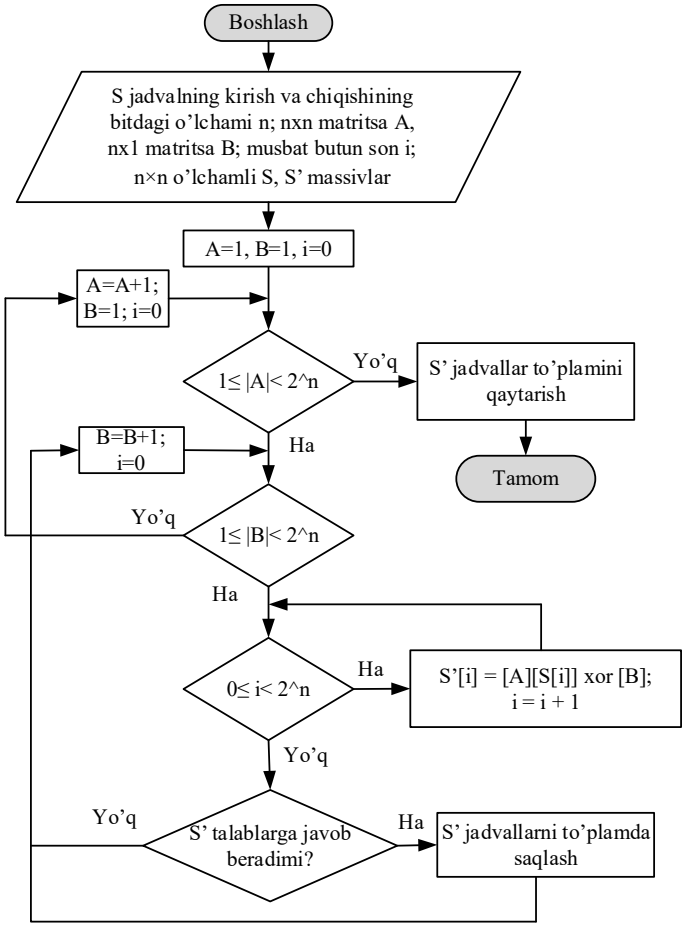
Generatsiya qilingan S jadvallarni yuqorida keltirilgan kengaytirilgan umumiy talablar bo‘yicha baholash natijalari 5-jadvalda keltirilgan. 5-jadvalda yangi S jadvallarni mavjudiga nisbatan yaxshi ko‘rsatkichga ega bo‘lgan xususiyatlari belgilangan holda keltirilgan. S jadval nomi ustunidagi belgilangan yacheykalar esa mavjudlaridan bir necha xususiyat bo‘yicha ustunlikka ega S jadvallarni ko‘rsatadi.

Taklif etiladigan raund akslantirishlarida chiziqsiz amal sifatida foydalanish uchun tanlab olingan S jadvallar quyida keltirilgan:

S_Box1 (4×4) = (6, 10, 12, 1, 3, 15, 5, 2, 9, 4, 0, 7, 14, 8, 11, 13);

S_Box1 (5×5) = (6, 9, 27, 22, 17, 30, 13, 0, 25, 14, 5, 16, 31, 8, 2, 23, 19, 24, 10, 3, 4, 15, 28, 21, 20, 7, 12, 29, 18, 1, 11, 26);

S_Box21 (6×6) = (40, 13, 24, 53, 21, 34, 1, 62, 59, 18, 9, 44, 36, 29, 50, 7, 33, 11, 30, 57, 47, 23, 54, 3, 48, 14, 38, 17, 42, 4, 26, 61, 63, 22, 6, 39, 52, 10, 45, 27, 19, 43, 12, 56, 28, 49, 35, 2, 0, 46, 51, 16, 25, 32, 8, 60, 55, 20, 15, 37, 31, 41, 5, 58).



3-rasm. S jadvaldan affin akslantirishi yordamida yangi S jadvalni hosil qilish algoritmining blok sxemasi

Mazkur bobning 2.3-paragrafida 256, 320 va 384 bitli holat ($S = S_r \parallel S_c$) uzunligiga ega raund akslantirishlari ishlab chiqilgan bo‘lib (mos ravishda P256, P320 va P384 shartli nomlar bilan belgilanadi), ular umumiy holda quyidagicha ifodalanadi:

$$p = p_L \cdot p_S \cdot p_C$$

bu yerda, p_L – chiziqli bosqichni, p_S – chiziqsiz bosqichni va p_C – raund o‘zgarmaslarini qo‘shish bosqichini anglatib, ular quyida batafsil keltirilgan.

Chiziqli bosqich p_L. Chiziqli bosqich 64 bitli so‘zlar ustida siklik siljitish va XOR amalida qo‘shishdan iborat bo‘lib, nafaqat so‘z ichida balki, so‘zlar orasida ham aralashtirishni amalga oshiradi. Ushbu ifodalar, 256 bitli ($i \in [0,3]$ va $n = 4$), 320 bitli ($i \in [0,4]$ va $n = 5$) va 384 bitli ($i \in [0,5]$ va $n = 6$) holat uchun quyidagi tenglikdan foydalaniladi:

$$x'_i \leftarrow x_i \oplus (x_i \ggg C1_i) \oplus (x_i \ggg C2_i) \oplus (x_{(i+1) mod\ n} \ggg 11)$$

bu yerda, $C1 = \{7,15,2,18,9,17\}$ va $C2 = \{36,52,25,44,60,35\}$ ga teng. So‘z ichida va so‘zlar orasida aylantirish qiymatlari maksimal aralashtirish imkoniyatini yaratish va kam harajatli amalga oshirish nuqtai nazaridan tanlandi. Ushbu chiziqli akslantirishning tarmoqlanishlar soni ham 5 ga teng bo‘lib, 3-raunddan so‘ng maksimal aralashtirish ko‘rsatkichiga erishadi.

Chiziqsiz bosqich p_S. Ushbu bosqich akslantirishning muhim bosqichi bo‘lib, unda 256 bitli holat uchun 4×4 o‘lchamli S jadvaldan, 320 bitli holat uchun

5×5 o‘lchamli S jadvaldan, 384 bitli holat uchun 6×6 o‘lchamli S jadvaldan foydalaniladi. Ushbu S jadvallar yuqorida keltirildi.

5-jadval

Mavjud S jadvallar asosida yangi hosil qilinganlarining kengaytirilgan umumiy kriptografik talablar bo‘yicha baholash natijalari

S jadval nomi	Umumiy					Chiziqli				Differensiyal			Alg	DPA			Ama
	B+	FP↓	OFP↓	SAC (=0.5)	BIC-SAC (=0.5)	NL↑	LP↓	CI↑	LBN↑	DP↓	PC↑	DBN↑	AI, TS↑	TO↓	CCV↑	SNR↓	ME↓
4x4 S jadvallar																	
Present	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
S_Box1	+	0	0	0.625	0.562	4	0.25	0,1,0,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	14
S_Box2	+	0	0	0.625	0.562	4	0.25	0,0,1,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	15
S_Box3	+	0	0	0.625	0.562	4	0.25	0,0,1,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	14
5x5 S jadvallar																	
Ascon	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.322	0.501	3.015	20
S_Box1	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box2	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box8	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box14	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box18	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
6x6 S jadvallar																	
S_Box0	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.599	0.339	4.341	44
S_Box21	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.539	0.447	3.929	43
S_Box23	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.583	0.423	4.010	43
S_Box26	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.583	0.542	3.646	44

Raund o‘zgarmaslarini qo‘shish p_C. Raund akslantirishi uchun raund o‘zgarmaslarini hosil qilish chiziqli teskari aloqali siljitish registoriga asoslangan yondashuvdan foydalanildi. Buning uchun $p(x) = x^8 + x^6 + x^5 + x^4 + 1$ primitiv ko‘phadidan foydalanildi. Bundan tashqari, hosil bo‘lgan qiymatlarning Hemming salmog‘i kamida 4 ga teng bo‘lishi talabini inobatga olgan holda, 0x0d (13), 0x0e (14), 0x0f (15), 0x15 (21) va 0x3b (59) kabi dastlabki qiymatlar (seed) bilan ishga tushirish talab etiladi.

Dissertatsiyaning **“Yengil vaznli autentifikatsiyalangan shifrlash algoritmlari”** deb nomlanuvchi uchinchi bobida 320 va 384 bitli holatga ega sponge konstruksiyasi uchun raund akslantirishlarini yaratish, ular asosida yengil vaznli simmetrik blokli autentifikatsiyalangan shifrlash algoritmlarini qurish masalasiga to‘xtalib o‘tilgan.

Ushbu bobda taklif etiladigan AEAD turidagi shifrlash algoritmlari P320 va P384 akslantirishlariga asoslangan bo‘lib, ularni umumiy parametrlari 6-jadvalda keltirilgan. Bu yerda, kalit uzunligi (k), blok uzunligi (r) hamda ichki raund qiymatlari, a va b, bilan ifodalangan. Shuningdek, bir martali foydalaniladigan qiymat (nonce) N, o‘zgaruvchan uzunlikdagi aloqador ma’lumot (AD) A, autentifikatsiya tegi T va boshlang‘ich vektor (Initialization vector, IV). Shundan kelib chiqib, shifrlash funksiyasini $E_{k,r,a,b}(K, N, A, P) = (C, T)$ shaklida va unga mos rasshifrovkalash funksiyasini $D_{k,r,a,b}(K, N, A, C, T) \in \{P, \perp\}$ kabi belgilash mumkin. Bu yerda, C shifrmatn hamda rasshifrovkalashda autentifikatsiya tegi to‘g‘ri bo‘lganda ochiqmatn P ni, aks holda xatolik $\perp$ ni qaytariladi.

6-jadval

Taklif etilayotgan AEAD algoritmlari uchun parametrlar

Nomi	Algoritmlar	k, bit	nonce, bit	teg, bit	b, bit	c, bit	IV, bit	A, bit	r, bit	Raundlar soni		Xavfsizlik darajasi
										a	b	
AEAD-P320	$E, D_{128,64,12,6}$	128	128	128	320	256	64	$\{0,1\}^*$	64	12	6	128
AEAD-P384	$E, D_{128,128,14,8}$	128	128	128	384	256	128	$\{0,1\}^*$	128	14	8	128
AEAD-P384a	$E, D_{192,128,14,8}$	192	128	128	384	256	64	$\{0,1\}^*$	128	14	8	128

Barcha AEAD-P320, AEAD-P384 va AEAD-384a shifrlar umumiy holda 1-algoritm asosida ishlaydi. Mazkur algoritmda parametrlarni o‘zgartirish orqali AEAD-P320, AEAD-P384 va AEAD-384a shifrlash rejimlarini osonlik bilan loyihalash mumkin.

1-algoritm. AEAD-P320, AEAD-P384 va AEAD-384a shifrlarining protseduralari

Autentifikatsiyalovchi shifrlash	**Tekshirilgan rasshifrovka qilish**
Kirish: ochiq matn $P \in \{0,1\}^*$, kalit $K \in \{0,1\}^k$, Nonce $N \in \{0,1\}^{128}$, aloqador ma’lumot $A \in \{0,1\}^*$ **Chiqish:** shifrmatn $C \in \{0,1\}^{\lvert P\rvert}$, teg $T \in \{0,1\}^{128}$	**Kirish:** ochiq matn $P \in \{0,1\}^*$, kalit $K \in \{0,1\}^k$, Nonce $N \in \{0,1\}^{128}$, aloqador ma’lumot $A \in \{0,1\}^*$, teg $T \in \{0,1\}^{128}$ **Chiqish:** ochiqmatn $P \in \{0,1\}^{\lvert C\rvert}$ yoki $\perp$

Initsializatsiya
$S \leftarrow IV_{k,r,a,b} \parallel K \parallel N$
$S \longleftarrow p^a(S) \oplus (0^{b-k} \parallel K)$
Aloqador ma’lumotni ishlash
agar $\lvert A\rvert > 0$ **u holda**
$A_1 \dots A_s \leftarrow A \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, s$ **do**
$S \leftarrow p^b(S_r \oplus A_i \parallel S_c)$
$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
Ma’lumotni ishlash
$P_1 \dots P_t \leftarrow P \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, t-1$ **do**
$S_r \leftarrow S_r \oplus P_i$
$C_i \leftarrow S_r$
$S \longleftarrow p^b(S)$
$S_r \leftarrow S_r \oplus P_t$
$\hat{C}_t \leftarrow \lfloor S_r \rfloor_{\lvert P\rvert \bmod r}$
Yakunlash
$S \longleftarrow p^a(S \oplus (0^r \parallel K \parallel 0^{c-k})$
for $i = 1, \dots, d = \lvert T\rvert / r$ **do**
$S \longleftarrow p^a(S)$
$T_i \longleftarrow S_r$
return $C_1 \parallel \cdots \parallel C_{t-1} \parallel \hat{C}_t, T$
	Initsializatsiya
	$S \leftarrow IV_{k,r,a,b} \parallel K \parallel N$
	$S \longleftarrow p^a(S) \oplus (0^{b-k} \parallel K)$
	Aloqador ma’lumotni ishlash
	agar $\lvert A\rvert > 0$ **u holda**
	$A_1 \dots A_s \leftarrow A \parallel 1 \parallel 0^* \parallel 1$
	for $i = 1, \dots, s$ **do**
	$S \leftarrow p^b(S_r \oplus A_i \parallel S_c)$
	$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
	Shifrmatnni ishlash
	$C_1 \dots C_{t-1} \hat{C}_t \leftarrow C, 0 \le \lvert \hat{C}_t \rvert < r$
	for $i = 1, \dots, t-1$ **do**
	$P_i \leftarrow S_r \oplus C_i$
	$S \leftarrow C_i \parallel S_c$
	$S \longleftarrow p^b(S)$
	$\hat{P}_t \leftarrow \lfloor S_r \rfloor_{\lvert \hat{C}_t \rvert} \oplus \hat{C}_t$
	$S_r \leftarrow S_r \oplus (\hat{P}_t \parallel 1 \parallel 0^* \parallel 1)$
	Yakunlash
	$S \longleftarrow p^a(S \oplus (0^r \parallel K \parallel 0^{c-k})$
	for $i = 1, \dots, d = \lvert T\rvert / r$ **do**
	$S \longleftarrow p^a(S)$
	$T^*{}_i \longleftarrow S_r$
	agar $T = T^*$ **return** $P_1 \parallel \cdots \parallel P_{t-1} \parallel \hat{P}_t$ **aks holda return** $\perp$

Barcha algoritm variantlarida dastlabki holat (320 yoki 384 bitli) k bitli kalit K, 128 bitli nonce N va algoritm parametrlarini ifodalovchi 64 bitli (AEAD-P320 uchun) yoki 128 bitli quyidagi boshlang‘ich vektor yordamida shakllantiriladi:

$$IV_{k,r,a,b} \leftarrow k \parallel r \parallel a \parallel b \parallel 10^*1$$
$$= \begin{cases} 80400c0680000001 & AEAD-P320\ uchun \\ 80800e0880000000000000000000000001 & AEAD-P384\ uchun \\ c0800e0880000001 & AEAD-P384a\ uchun \end{cases}$$

Mazkur holda, dastlabki holat $S \longleftarrow IV_{k,r,a,b} \parallel K \parallel N$ ga teng bo‘ladi.

Dissertatsiyaning **“Yengil vaznli xesh funksiyani, psevdotasodifiy sonlar generatorini qurish usuli va algoritmlari”** deb nomlanuvchi to‘rtinchi bobida 320 va 384 bitli raund akslantirishlari asosida kalitli/ kalitsiz, o‘zgarmas/ o‘zgaruvchan uzunlikdagi xesh qiymatlarni hosil qilish usuli va algoritmlarini, 256 bitli raund akslantirishi asosida psevdotasodifiy sonlar generatorini qurish masalasi ko‘rib chiqilgan.

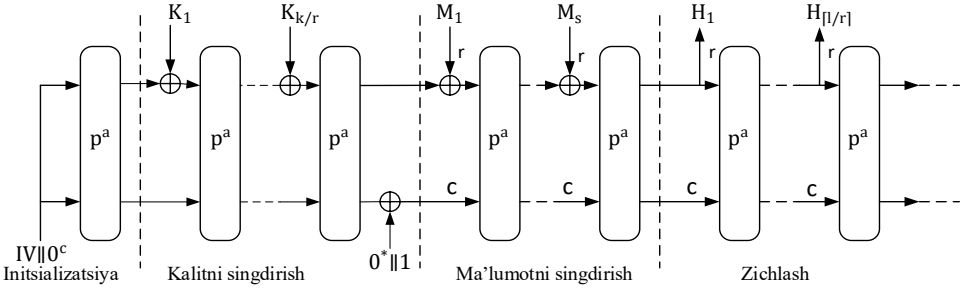
Ishlab chiqiladigan xesh funksiyalar sponge konstruksiyasiga asoslanib, holat uzunligi 320 va 384 bitga teng ikki akslantirishlar, mos holda P320 va P384 bilan yangilanadi. Umumiy holda ham kalitsiz ham kalitli xesh funksiyalarni, ham o‘zgarmas ham o‘zgaruvchan uzunlikdagi xesh qiymatlarni yagona ifodalashda kalit uzunligi k (agar kalitsiz rejim bo‘lsa $k = 0$), blok uzunligi (P320 akslantirish uchun 64 bit va P384 akslantirishi uchun 128) r, xesh qiymat uzunligi h (agar o‘zgaruvchan uzunlik bo‘lganda $h = 0$) va raundlar soni a parametrlardan foydalaniladi. Shundan kelib chiqib, taklif etilayotgan xesh funksiyalar $X_{k,r,a,h}$ o‘zgaruvchan uzunlikdagi kiruvchi xabar ma’lumoti M va kalit K ni chiqishda uzunligi $l \leq h$ bo‘lgan H ga akslantirib beradi:

$$X_{k,r,a,h}(K, M, l) = H.$$

O‘zgarmas uzunlikdagi xesh funksiya variantlari uchun $h = 256$ ga teng bo‘lsa, o‘zgaruvchan uzunlikdagi variantlar uchun $h = 0$ ga teng bo‘ladi. Mos holda, kalitli rejimda kalitlar 128 yoki 192 ga teng bo‘ladi, kalitsiz rejimda esa $k = 0$ ga teng bo‘ladi.

Taklif etilayotgan xeshlash algoritmlarining nomi va kalit uzunligi k, blok uzunligi r, xesh qiymat uzunligi h, algoritmning barcha bosqichlari uchun akslantirishning raundlar soni a, boshlang‘ich vektor IV, akslantirishlardagi holat uzunligi b, sig‘im uzunligi c va xavfsizlik darajasi haqida ma’lumotlar 7-jadvalda keltirilgan. Nomlanishdagi “K” harfi bilan boshlangan variantlar kalitli rejim ekanligini va “HASH” jumlasining borligi xesh funksiya o‘zgarmas uzunlikdagi, “XOF” (Extended output function, Xof) jumlasining borligi esa o‘zgaruvchan uzunlikdagi xesh qiymatni hosil qiluvchi variant ekanligini ifodalaydi.

Har ikkala akslantirish asosida ishlab chiqiladigan kalitli xesh funksiyalarni qurish usulining sxemasi 4-rasmda tasvirlangan.



4-rasm. Kalitli rejimdagi xesh funksiyalarni qurish usulining sxemasi

7-jadval

Taklif etilayotgan xesh funksiya algoritmlari uchun parametrlar

Algoritm nomi	Holat, b, bit	Sig‘im, c, bit	IV, bit	k, bit	h, bit	r, bit	a	Xavfsizlik darajasi, bit
KHASH-P320	320	256	64	128	256	64	12	128
KHASH-P320a	320	256	64	192	256	64	12	128
KXOF-P320	320	256	64	128	0	64	12	$min\,(128, l/2)$
KXOF-P320a	320	256	64	192	0	64	12	$min\,(128, l/2)$
KHASH-P384	384	256	128	128	256	128	14	128
KHASH-P384a	384	256	128	192	256	128	14	128
KXOF-P384	384	256	128	128	0	128	14	$min\,(128, l/2)$
KXOF-P384a	384	256	128	192	0	128	14	$min\,(128, l/2)$
HASH-P320	320	256	64	0	256	64	12	128
XOF-P320	320	256	64	0	0	64	12	$min\,(128, l/2)$
HASH-P384	384	256	128	0	256	128	14	128
XOF-P384	384	256	128	0	0	128	14	$min\,(128, l/2)$

Barcha kalitli xesh funksiya algoritmlari umumiy holda quyidagi 2-algoritm asosida ishlaydi. Mos holda barcha kalitsiz xesh funksiya algoritmlari umumiy holda quyidagi 3-algoritm asosida ishlaydi.

2-algoritm. Kalitli xesh funksiya algoritmlarining protsedurasi	**3-algoritm. Kalitsiz xesh funksiya algoritmlarining protsedurasi**
Kirish: xabar $M \in \{0,1\}^*$, kalit $K \in \{0,1\}^k$, chiquvchi bit o‘lchami $l = h$ yoki o‘zgaruvchan qiymat uchun $h = 0$ **Chiqish:** xesh qiymat $H \in \{0,1\}^l$	**Kirish:** xabar $M \in \{0,1\}^*$, chiquvchi bit o‘lchami $l = h$ yoki o‘zgaruvchan qiymat uchun $h = 0$ **Chiqish:** xesh qiymat $H \in \{0,1\}^l$

Initsializatsiya
$S \leftarrow p^a(IV_{k,r,a,h} \parallel 0^c)$
Kalitni singdirish
$K_1 \dots K_d \leftarrow K \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, d$ do
$S \leftarrow p^a(S_r \oplus K_i \parallel S_c)$
$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
Ma’lumotni singdirish
$M_1 \dots M_s \leftarrow M \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, s$ do
$S \leftarrow p^a(S_r \oplus M_i \parallel S_c)$
Zichlash
for $i = 1, \dots, t = \lceil l/r \rceil$ do
$H_i \leftarrow S_r$
$S \leftarrow p^a(S)$
return $\lfloor H_1 \parallel \cdots \parallel H_t \rfloor_l$
	Initsializatsiya
	$S \leftarrow p^a(IV_{k,r,a,h} \parallel 0^c)$
	Singdirish
	$M_1 \dots M_s \leftarrow M \parallel 1 \parallel 0^* \parallel 1$
	for $i = 1, \dots, s$ do
	$S \leftarrow p^a(S_r \oplus M_i \parallel S_c)$
	Zichlash
	for $i = 1, \dots, t = \lceil l/r \rceil$ do
	$H_i \leftarrow S_r$
	$S \leftarrow p^a(S)$
	return $\lfloor H_1 \parallel \cdots \parallel H_t \rfloor_l$

Xesh funksiyalarning barcha P320 akslantirishga asoslangan variantlari uchun boshlang‘ich vektor IV 64-bit uzunlikka ega bo‘lib, kalit va kalitsiz rejimlar uchun quyidagicha hisoblanadi: $IV_{k,r,a,h} \leftarrow k \parallel r \parallel a \parallel h \parallel 10^*1$, bu yerda, k, r, a – lar uchun bir bayt, h uchun esa 2 bayt ajratilgan.

Shunga mos holda, P384 akslantirishiga asoslangan barcha xesh funksiya variantlari uchun boshlang‘ich vektorlar quyidagicha hisoblanadi: $IV_{k,r,a,h} \leftarrow k \parallel r \parallel a \parallel h \parallel 10^*1$, bu yerda, k, r, a – lar uchun bir bayt, h uchun esa 2 bayt ajratilgan.

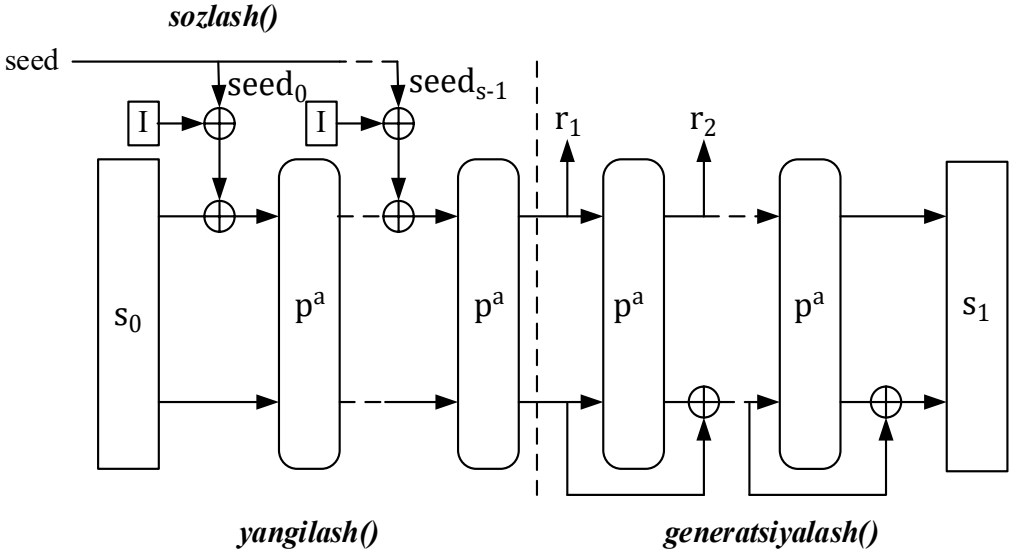
Shuningdek, 4.3-paragrafda P256 akslantirish asosida psevdotasodifiy sonlarni generatsiyalash (PTSG) algoritmi ishlab chiqilgan. PTSGni qurish uchun foydalanilgan parametrlar 8-jadvalda keltirilgan bo‘lib, algoritm holatni qayta tiklash hujumiga 2^{128} qarshilikka ega.

8-jadval

PTSG uchun tavsiya etilgan parametrlar (bitda)

Holat, b	Sig‘im, c	Ma’lumot bloki, r	r bitli seed bloklar soni, s	Entropiya, I	Raundlar soni, p^a
256	128	128	2	128	12

Keltirilgan parametrlar asosida PTSGning umumiy ko‘rinishi 5-rasmda keltirilgan bo‘lib, u holatni *sozlash()*, *yangilash()* va psevdotasodifiy qiymatlarni *generatsiyalash()* bosqichlaridan iborat.



5-rasm. Sponge konstruksiyasiga asoslangan PTSGning umumiy ko‘rinishi

Taklif etilgan PTSG algoritmini NIST statistik testlar to‘plami yordamida baholash ikki sharoitda amalga oshirildi. Birinchi sharoitda, ishlab chiqilgan dasturiy vosita yordamida turli seed va entropiya qiymatlaridan 2 million (2×10^6) bitdan iborat 100 ta psevdotasodifiy ketma-ketliklar (jami 2×10^8 bit) to‘plami hosil qilindi. Ikkinchi sharoitda esa yagona seed va entropiya orqali 2×10^8 bit hosil qilinib, 2×10^6 bitdan bo‘lgan 100 ta qismga ajratildi. Tahlil natijasida birinchi sharoitda 96.7%, ikkinchi sharoitda esa 97.3% bilan tasodifiylik testlaridan o‘tgan.

Dissertatsiyaning **“Yengil vaznli simmetrik kriptografik algoritmlarni kriptotahlilga baholash va amalga oshirish natijalari”** deb nomlanuvchi

beshinchi bobida ishlab chiqilgan yengil vaznli kriptografik algoritmlarni (chiziqli, integral va algebraik) kriptotahlil usullariga baholash, turli imkoniyatli qurilmalarda dasturiy amalga oshirish natijalari hamda dasturiy vositalarni amaliyotda tatbiq etishdan olingan natijalar bayon etilgan.

Xususan, P256 akslantirishining chiziqli kriptotahlil natijasi unga asoslangan barcha algoritmlarni 3-raunddan boshlab chiziqli kriptotahlilga bardoshli ekanligini ko‘rsatdi. Mazkur xulosani P320 va P384 akslantirishlari uchun ham aytish mumkin.

Algoritmlarning algebraik kriptotahlil natijalari esa shakllantiriladigan tenglamalar soniga nisbatan tenglamalarning darajalari, tenglamalar sistemasidagi birhadlar soni va yechish murakkabligi yuqoriligi sababli 5 raundli P256, P320 va P384 akslantirishlar algebraik kriptotahlil usuliga bardoshli ekanligini ko‘rsatdi.

Shuningdek, algoritmlar integral kriptotahlil usulida ham baholandi. Baholash natijalari 7 raundli holatdan keyin 3-raund S jadvalining kirishigacha teskari akslantirishlarni bajarish imkonining yo‘qligi va talab qilinadigan tanlashlar sonini amalga oshirishning murakkabligi sababli, 256 bitli algoritmni 8-raunddan boshlab, 320 bitli va 384 bitli algoritmlarni 7-raunddan boshlab integral kriptotahlil usuliga bardoshligini ko‘rsatdi.

Taklif etilgan barcha yengil vanzli kriptografik algoritmlar quyida keltirilgan muhitlarda ishlash tezligi bo‘yicha sinovdan o‘tkazildi va natijalar 9-jadvalda keltirilgan.

9-jadval

Ishlab chiqilgan algoritmlarni dasturiy amalga oshirish natijalari

Nomi	Algoritmlar	Shifrlash/ deshifrlash/ xeshlash/ generatsiyalash tezligi, Mbayt/ sek		
		1-muhit	2-muhit	3-muhit
AEAD-P320	$E, D_{128,64,12,6}$	257.149/ 246.810	41.306/ 41.322	345.620/ 340.691
AEAD-P384	$E, D_{128,128,14,8}$	212.981/ 217.124	36.367/ 36.533	336.095/ 333.150
AEAD-P384a	$E, D_{192,128,14,8}$	214.359/ 215.879	35.956/ 36.247	336.143/ 331.733
KHASH-P320	$X_{128,\ 64,12,256}$	125.057	20.785	175.373
KHASH-P320a	$X_{192,\ 64,12,256}$	129.995	20.788	175.283
KXOF-P320	$X_{128,\ 64,12,0}$	132.578	20.692	176.411
KXOF-P320a	$X_{192,\ 64,12,0}$	132.822	20.697	176.611
KHASH-P384	$X_{128,128,14,256}$	130.476	21.372	194.408
KHASH-P384a	$X_{192,128,14,256}$	129.938	21.374	193.306
KXOF-P384	$X_{128,\ 128,14,0}$	131.730	21.373	194.414
KXOF-P384a	$X_{192,\ 128,14,0}$	130.390	21.375	193.283
HASH-P320	$X_{0,\ 64,12,256}$	130.305	20.787	175.390
XOF-P320	$X_{0,\ 64,12,0}$	132.378	20.690	176.548
HASH-P384	$X_{0,128,14,256}$	131.680	21.373	194.875
XOF-P384	$X_{0,\ 128,14,0}$	129.887	21.372	192.941
PRNG-P256	$X_{256,\ 128,128,12}$	267.798	53.932	344.813

Muhit 1: Intel(R) Core(TM) i5-10500T CPU @ 2.30GHz, 16,0 GB (15,7 GB usable), 64-bit operating system, x64-based processor, Windows 11 Pro, 24H2, mingw-gcc).

Muhit 2: Rasberry Pi 4 (4GB RAM, 64-bit quad-core Cortex-A72 processor, 2.2 GHz, Raspberry Pi reference 2025-05-13, Debian GNU/Linux 12 (bookworm), C dasturlash tili, gcc 12.2.0).

Muhit 3: Ubuntu 22.04.5 LTS, CPU: Intel(R) Core(TM) i5-1334U, RAM: 8 Gb, SSD 256, gcc.

Shuningdek, dasturiy vositalar Atmega 328P (ROM: 32 Kbayt, RAM: 2 Kbayt, chastota: 16 Mhz, tok kuchi: 5 V - 16 Mhz da 9.2 mA.) 8 bitli mikrokontrollerida amalga oshirildi. 10-jadvalda algoritmlarni amalga oshirishda talab etilgan ROM, RAM xotira hajmlari, keltirilgan uzunlikdagi ma'lumotlar uchun jarayon vaqti va talab etgan energiya sarfi haqidagi ma'lumotlar keltirilgan.

10-jadval

Ishlab chiqilgan algoritmlarni apparat-dasturiy amalga oshirish natijalari

Nomi	Parametrlar	Bayt		Bayt, (AD:M=(128:128)), (M=512, h=32), (L=512)	
		ROM	RAM	Vaqt, µs	Energiya, mJ
AEAD-P320	$E, D_{128,64,12,6}$	10838	374	52329	2.407
AEAD-P384	$E, D_{128,128,14,8}$	14296	374	55965	2.427
AEAD-P384a	$E, D_{192,128,14,8}$	15344	382	56015	2.574
KHASH-P320	$X_{128,\ 64,12,256}$	4930	308	187547	8.627
KHASH-P320a	$X_{192,\ 64,12,256}$	4940	316	190153	8.747
KXOF-P320	$X_{128,\ 64,12,0}$	4890	284	187547	8.627
KXOF-P320a	$X_{192,\ 64,12,0}$	4900	292	190153	8.747
KHASH-P384	$X_{128,128,14,256}$	7038	308	171965	7.910
KHASH-P384a	$X_{192,128,14,256}$	7048	316	171965	7.910
KXOF-P384	$X_{128,\ 128,14,0}$	6550	285	171965	7.910
KXOF-P384a	$X_{192,\ 128,14,0}$	6560	293	171965	7.910
HASH-P320	$X_{0,\ 64,12,256}$	4570	292	182334	8.387
XOF-P320	$X_{0,\ 64,12,0}$	4514	268	182334	8.387
HASH-P384	$X_{0,128,14,256}$	6424	292	167316	7.697
XOF-P384	$X_{0,\ 128,14,0}$	5906	269	167316	7.697
PRNG-P256	$X_{256,\ 128,128,12}$	5530	284	70953	3.264

Bundan tashqari, ishlab chiqilgan yengil vaznli kriptografik algoritmlar Arduino Mega (8 bitli, Atmega-2560, ROM = 253952 bayt, RAM = 8192 bayt, 16 Mhz, 5 V, 20.2 mA), Arduino Leonardo (8 bitli, ATmega32u4, ROM = 28672 bayt, RAM = 2560 bayt, 16 Mhz, 5 V, 12.8 mA) va Arduino DUE (32 bit, Atmel SAM3X8E ARM Cortex-M3 CPU, 84 Mhz, 3.3 V, 60 mA) mikrokontrollerlarida amalga oshirildi hamda tegishli natijalar olindi. Olingan natijalar ishlab chiqilgan yengil vaznli kriptografik algoritmlarni imkoniyati cheklangan muhitlarda foydalanish mumkinligini ko'rsatdi.

XULOSA

“Buyumlar interneti tizimida axborotni kriptografik himoyalash usullari va algoritmlari” mavzusidagi dissertatsiya ishida olib borilgan tadqiqot natijalari asosida quyidagi xulosalar taqdim etildi:

1. Keng tarqalgan yengil vaznli kriptografik algoritmlardagi turli o‘lchamli chiziqsiz akslantirishlar kengaytirilgan umumiy kriptografik talablar asosida baholandi. Baholash natijalari ularni apparat amalga oshirishdagi va yon-kanal hujumlariga bardoshlik natijalari eng yaxshi emasligini ko‘rsatdi.
2. Kengaytirilgan sinus va tent funksiyalaridan kombinatsion tarzda foydalanish orqali xaotik akslantirishlarga asoslangan turli o‘lchamli S jadvallarni hosil qilish usuli takomillashtirilgan. Takomillashtirilgan usul asosida ishlab chiqilgan algoritm orqali hosil qilingan 4×4, 5×5, 6×6 va 8×8 o‘lchamli S jadvallar yuqori kriptografik talablarni qanoatlantirishi aniqlandi.
3. Affin akslantirishini kriptografik algoritmning chiziqsiz sath xususiyatlariga ta’sirini o‘rganish asosida yon-kanal hujumlariga bardoshli, apparat tarzda amalga oshirishga qulay S jadvallarni hosil qilish algoritmi ishlab chiqildi. Ishlab chiqilgan chiziqsiz akslantirishlarni hosil qilish algoritmi yordamida hosil qilingan 4×4, 5×5 va 6×6 o‘lchamli S jadvallar qolgan xususiyatlarni saqlab qolganda mavjudlaridan apparat amalga oshirilishdagi kam sonli mantiqiy elementlarni talab etishi, yon-kanal hujumiga mavjudlaridan ko‘ra yuqori bardoshlikni ta’minlashi tajribalar orqali ko‘rsatildi.
4. Turli holat uzunlikli raund akslantirishlariga ega sponge konstruksiyasi asosida ma’lumotlarni autentifikatsiyalovchi shifrlash imkoniyatli kriptografik algoritmlar ishlab chiqildi. Ishlab chiqilgan barcha algoritmlar konstruksiyaga qaratilgan umumiy hujumga nisbatan 128 bitli bardoshlikni ta’minlab, AEAD_P320 algoritmi qolganlariga qaraganda eng yuqori (o‘rtacha 345.62 MB/s) tezlikni qayd etgan.
5. Turli holat uzunlikli raund akslantirishlariga ega sponge konstruksiyasi asosida ma’lumotlarni kalitli va kalitsiz xeshlab, o‘zgaruvchan hamda o‘zgarmas uzunlikdagi xesh qiymatlarni hosil qiluvchi kriptografik usul va algoritmlar ishlab chiqildi. Ishlab chiqilgan o‘zgarmas uzunlikdagi (256 bit) xesh qiymatni hosil qiluvchi barcha algoritmlar 128 bitli bardoshlilikni, o‘zgaruvchan uzunlikdagi (l bit) xesh qiymatni hosil qiluvchi barcha algoritmlar esa $min\,(128, l/2)$ munosabatli bardoshlilikni ta’minlab, 128 bitli xesh qiymatni hosil qilishda HASH_P384 algoritmi eng yuqori (o‘rtacha 194.875 MB/s) tezlikni qayd etgan.
6. Sponge konstruksiyasi asosida mukammal xavfsizlikni ta’minlovchi psevdotasodifiy sonlarni hosil qilish algoritmi ishlab chiqildi. Ishlab chiqilgan PTSGning NIST statistik testlar to‘plami orqali olingan natijalari o‘rtacha 97.3% tasodifiylik darajasini ko‘rsatib, psevdotasodifiy qiymatlarni hosil qilishda o‘rtacha 344.813 MB/s tezlikni qayd etgan.
7. Ishlab chiqilgan yengil vaznli kriptografik algoritmlar qurilish xususiyatiga ko‘ra umumiy kriptotahlil usullariga, raund akslantirishlari xususiyatiga ko‘ra chiziqli, algebraik va integral kriptotahlil usullariga baholandi. Baholash natijalari algoritmlarni chiziqli kriptotahlilga 3-raunddan boshlab,

algebraik kriptotahlilga 5-raunddan va integral kriptotahlilga esa 7-raunddan boshlab bardoshlikni ta’minlashini ko‘rsatdi.

8. Ishlab chiqilgan yengil vaznli kriptografik algoritmlar bir qancha 8 bitli imkoniyati cheklangan buyumlar interneti qurilmalarida sinovdan o‘tkazildi. Arduino Mega platasida olib borilgan sinov natijalari shifrlash algoritmlari 8% gacha ROM xotira hajmini, 11% gacha RAM xotira hajmini, psevdotasodifiy sonlarni generatsiyalash algoritmi esa 3% gacha ROM xotira hajmini, 5% gacha RAM xotira hajmini, xesh funksiya algoritmlari esa 3% gacha ROM xotira hajmini, 10% gacha RAM xotira hajmini talab etishini ko‘rsatdi.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.02
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ХУДОЙКУЛОВ ЗАРИФЖОН ТУРАКУЛОВИЧ

МЕТОДЫ И АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ИНТЕРНЕТА ВЕЩЕЙ

05.01.05 - Методы и системы защиты информации. Информационная безопасность

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ТЕХНИЧЕСКИХ НАУК (DSc)**

Ташкент-2025

Тема диссертации доктора технических наук (DSc) зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за №B2025.3.DSc/T982.

Диссертация выполнена в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещён на веб-сайте Научного совета (www.tuit.uz) и на информационно-образовательный портале (www.ziyonet.uz) «ZiyoNet».

Научный консультант:	**Ганиев Салим Каримович** доктор технических наук, профессор
Официальные оппоненты:	**Керимов Камил Фикратович** доктор технических наук, профессор
	Жураев Гайрат Умарович доктор физико-математических наук, профессор
	Курязов Давлатер Матякубович доктор физико-математических наук
Ведущая организация:	**Национальный университет Узбекистана имени Мирзо Улугбека**

Защита диссертации состоится «__» _____ 20__ года в ___ часов на заседании Научного совета DSc.13/30.12.2019.T.07.02 при Ташкентском университете информационных технологий. (Адрес: 100084, г.Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий (регистрационный номер №___). (Адрес: 100084, г.Ташкент, ул. Амир Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «__» _____ 20__ года.
(протокол рассылки №____ от «___» _____ 20__ года)

Б.Ш. Махкамов
Председатель Научного совета по присуждению ученых степеней, доктор экономических наук, профессор

М.С. Саиткамолов
Ученый секретарь Научного совета по присуждению ученых степеней, доктор экономических наук, доцент

Д.Я. Иргашева
Председатель Научного семинара при Научном совете по присуждению ученых степеней, доктор технических наук, профессор

ВВЕДЕНИЕ (аннотация докторской диссертации (DSc))

Актуальность и востребованность темы диссертации. В мире стремительное внедрение устройств Интернета вещей (Internet of Things, IoT) в информационно-коммуникационные инфраструктуры приводит к повышению эффективности и снижению эксплуатационных расходов, а также вызывает резкое увеличение проблем информационной безопасности. По аналитическим данным медиаплатформы «IoTforAll», в среднем на устройства Интернета вещей ежемесячно совершается 5400 атак, при этом стоимость успешной атаки превышает 330 000 долларов США, а ожидаемый ущерб от киберпреступлений к 2025 году превысит 10 триллионов долларов США.[1] Поскольку устройства Интернета вещей могут взаимодействовать с другими системами в информационно-коммуникационных инфраструктурах, обеспечение безопасности при передаче и хранении данных имеет важное значение. Поэтому сегодня особое внимание уделяется разработке методов и алгоритмов защиты, обеспечивающих безопасность передачи и хранения данных, подходящих для устройств Интернета вещей.

Во всем мире ведутся научные и практические исследования, направленные на изучение проблем информационной безопасности в среде Интернета вещей и разработку надежных механизмов защиты от угроз. В связи с этим особое внимание уделяется исследованиям, направленным на разработку криптографических методов и алгоритмов обеспечивающих конфиденциальность, целостность информации и аутентификацию источника сообщений, на адаптацию существующих алгоритмов, на оценку их с помощью методов криптоанализа и реализацию в программном и аппаратном виде, предназначенных для устройств IoT с ограниченными вычислительными и энергетическими возможностями. В результате проведённых в данной области научных исследований, конкурсов (NIST LWC), проектов (CAESAR, eSTREAM) и процессов стандартизации (ISO/IEC 29192) были разработаны международные и национальные стандартные криптографические алгоритмы, предназначенные для IoT-устройств, рекомендованные к использованию криптографические алгоритмы, а также они были оценены методами криптоанализа и приняты к применению.

В нашей стране в рамках стратегии «Цифровой Узбекистан – 2030», включающей комплексные меры по активному развитию цифровой экономики, широкому внедрению современных информационно-коммуникационных технологий во все отрасли и сферы, в первую очередь в государственное управление, образование, здравоохранение и сельское хозяйство, выполняется множество задач по развитию электронного правительства, цифровой индустрии, системы здравоохранения, промышленности и строительства, цифрового образования и цифровой инфраструктуры. Для эффективной организации выполнения данных задач, в частности при разработке систем умный город/умный дом с использованием IoT-устройств, при обеспечении постоянного мониторинга здоровья человека,

[1] https://www.iotforall.com/iot-telecom-vulnerabilities

а также при внедрении автоматизации процессов в промышленной сфере, целесообразно предотвращать возникающие проблемы информационной безопасности, своевременно реагировать на кибератаки, разрабатывать и внедрять надежные механизмы защиты информации.

Данное диссертационное исследование вносит вклад в реализацию задач, обозначенных в Законе Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764, Указе Президента Республики Узбекистан от 28 января 2022 года № УП-60 «О Стратегии развития нового Узбекистана на 2022-2026 годы», Постановлениях Президента Республики Узбекистан от 15 августа 2024 года № ПП-293 «О дополнительных мерах по развитию образования и науки в области криптологии в Республике Узбекистан», от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан» и других нормативно-правовых актах, касающихся данной деятельности.

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

Обзор научных исследований по теме диссертации. Научные исследования, направленные на разработку симметричных шифров, криптосистем с открытым ключом, электронных цифровых подписей, хеш-функций и генераторов псевдослучайных чисел, предназначенных для IoT-устройств, а также на совершенствование существующих алгоритмов и их оценку с использованием современных методов криптоанализа, проводились и продолжают проводиться в ведущих научных центрах и высших учебных заведениях мира. Примерами работ в этой области являются проект eSTREAM, реализуемый Европейским союзом по выбору подходящих алгоритмов для устройств Интернета вещей, проект CAESAR, реализуемый Международным обществом криптологических исследований, проект CRYPTREC, реализуемый Системой электронного правительства Японии, конкурс NIST LWC, проводимый Институтом NIST США, и серия стандартов ISO/IEC 29192.

Криптографические алгоритмы, работающие в устройствах Интернета вещей, характеризуются термином «легковесные» (lightweight), что обусловлено низкими вычислительными и энергетическими требованиями к этим алгоритмам. Научные исследования, направленные на создание легковесных симметричных криптографических алгоритмов, проводятся в самых передовых и ведущих научных исследовательских институтах, научно-исследовательских центрах и университетах мира, включая Институт NIST (США), Грацский технологический университет (Австрия), Infineon Technologies (Германия), Lamarr Security Research (Австрия), Университет Радбауда (Нидерланды), NTT (Nippon Telegraph and Telephone) (Япония), Рурский университет в Бохуме (Германия), Университет Карнеги-Меллона (США), Нанъянский технологический университет (Сингапур), Южный

федеральный университет (Российская Федерация), а также в нашей республике в Ташкентском университете информационных технологий имени Мухаммада ал-Хоразмий, Национальном университете Узбекистана имени Мирзо Улугбека, Центре научно-технических и маркетинговых исследований «UNICON.UZ» и Государственном унитарном предприятии «Центр кибербезопасности».

В мире только правительство США имеет собственный стандартный алгоритм (Ascon) для легковесной криптографии. В Республике Узбекистан в качестве алгоритма шифрования данных используется стандарт O‘zMSt 270:2024, а в качестве алгоритма функции хеширования - стандарт O‘zMSt 285:2024.

Степень изученности проблемы. На сегодняшний день вопросы разработки легковесных криптографических алгоритмов и их оценки методами криптоанализа рассмотрены в научных трудах ряда зарубежных ученых, среди которых: А.Богданов, К.Добрауниг, Дж.Дэймен, В.Реймен, Б.Гвидо, Дж.Бертони, Р.Болье, А.Е.Жуков, А.Люйкс, Н.Муха, Г.Цудик, Дж.Го, П.Дуонг, С.Хуан, Л.Янь, С.Баник, В.Чжан, Д.Гударзи, А.Канто, Д.Беллициа, З.Гун, К.Бейерле, А.Такор, Э.Андреева, З.Бао, Б.Бильгин, М.Хелл, Х.ВУ и другие.

Исследования, связанные с криптографическими методами защиты информации, такие как, разработка криптографических алгоритмов, их оценка методами криптоанализа и реализация в аппаратном и программном виде, проводятся со стороны таких ученых, как Й.Дэймен, В.Реймен, Б.Гвидо, Дж.Бертони, Б.Шнайер, К.Маккей, Э.К.Шеннон, К.Нюберг, Н.Т.Куртуа, Ж.Келси, К.Цантикиду, М.Дансари, М.Мацуи, Э.Ишукова, Л.Бабенко, П.Хасанов, М.Арипов, С.К.Ганиев, М.М.Каримов, Б.Ф.Абдурахимов, Д.Е.Акбаров, Г.Ю.Джураев, А.В.Кабулов, Д.М.Курьязов, Г.Н.Туйчиев, Х.Хасанов, О.Ахмедова, А.С.Атторов, Б.Ахмедов, И.М.Бойкузиев, О.М.Алланов, Р.Х.Алаев, М.А.Бердимуродов.

В то же время научных исследований по оценке нелинейных преобразований в распространенных легковесных криптографических алгоритмах для расширенных криптографических требований, разработке новых нелинейных преобразований, устойчивых к атакам по сторонним каналам и легко реализуемых на аппаратном уровне, а также по созданию легковесных симметричных криптографических алгоритмов и генераторов псевдослучайных чисел проведено недостаточно.

Связь диссертационного исследования с планами научно-исследовательских работ учреждения, в котором выполнена диссертация. Диссертационная работа выполнена в рамках плана научно-исследовательских работ Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий по проектам 598661-EPP-12018-1-RO-EPPKA2-CBHE-JP «Developing Services for Individuals with Disabilities – DECIDE» (2019–2022) и 10/18-F «Системная поддержка на основе создания научной лаборатории «Антивирусная защита» для разработки антивирусных программных средств и изучения вредоносных кодов» (2018–2020).

Цель исследования заключается в совершенствовании, разработке и оценке с помощью методов криптоанализа криптографических методов и алгоритмов, обеспечивающих информационную безопасность (конфиденциальность, целостность и аутентификацию источника), а также генерации псевдослучайных значений в устройствах с ограниченными возможностями.

Задачи исследования:

оценка S-таблиц различных размеров, используемых в современных легковесных криптографических алгоритмах, на основе расширенных общих криптографических требований;

совершенствование метода генерации S-таблиц различных размеров для использования в легковесных криптографических алгоритмах;

разработка легковесных алгоритмов аутентифицированного шифрования;

разработка методов и алгоритмов построения легковесных ключевых и бесключевых хэш-функций;

разработка легковесного алгоритма генератора псевдослучайных чисел;

проведение криптоанализа разработанных легковесных криптографических алгоритмов.

Объект исследования в качестве примера был взят процесс защиты информации на устройствах с ограниченными возможностями.

Предмет исследования составляет изучение криптографических методов и алгоритмов защиты информации на устройствах с ограниченными возможностями.

Методы исследования. В ходе исследования были использованы методы теории информации, теории вероятностей, теории множеств, дискретной математики, теории чисел, методы построения криптографических алгоритмов, методы оценки уровней безопасности криптографических алгоритмов, а также методы объектно-ориентированного программирования для реализации криптографических алгоритмов в виде программных средств.

Научная новизна исследования заключается в следующем:

оценены нелинейные преобразования различных размеров, применяемые в существующих лёгковесных криптографических алгоритмах, на основе расширенных общих криптографических требований, позволяющих проводить анализ с точки зрения безопасности;

усовершенствован метод генерации S-таблиц различных размеров с высокими показателями с точки зрения безопасности и аппаратной реализации посредством комбинационного использования расширенных синусоидальных и треугольных функций, а также разработан алгоритм генерации S-таблиц на основе улучшения свойств нелинейного слоя с помощью аффинных преобразований;

разработаны лёгковесные криптографические алгоритмы, обеспечивающие конфиденциальность и целостность данных, поддерживающие ключи и блоки различных размеров и позволяющие реализовать их в устройствах Интернета вещей;

разработаны лёгковесные криптографические методы и алгоритмы, обеспечивающие целостность данных и аутентификацию источника, поддерживающие формирование хеш-значений переменной и фиксированной длины и позволяющие реализовать их в устройствах Интернета вещей;

разработан лёгковесный криптографический алгоритм, обеспечивающий генерацию псевдослучайных последовательностей достаточной длины из единственного входного значения, позволяющий реализовать его в устройствах Интернета вещей и обеспечивающий высокий уровень безопасности;

оценена криптостойкость разработанных лёгковесных криптографических алгоритмов с использованием общих методов криптоанализа для определения уровня устойчивости их архитектуры и раундовых преобразований, а также с применением линейных, алгебраических и интегральных методов криптоанализа.

Практические результаты исследования заключаются в следующем:

разработано программное средство, оценивающее нелинейные преобразования различных размеров в распространенных легковесных криптографических алгоритмах на основе расширенных криптографических требований;

разработано программное средство для генерации S-таблиц различных размеров на основе комбинированного использования расширенных синусоидальных и треугольных хаотических преобразований;

разработано программное средство для формирования S-таблиц, устойчивых к атакам по побочным каналам и удобных для аппаратной реализации, на основе изучения влияния аффинных преобразований на свойства нелинейного слоя криптографических алгоритмов;

разработаны программные средства криптографических алгоритмов на основе sponge-конструкции с раундовыми преобразованиями различной длины состояния, обеспечивающие аутентифицированное шифрование данных;

разработаны программные средства криптографических алгоритмов на основе sponge-конструкции с раундовыми преобразованиями различной длины состояния, обеспечивающих ключевое и бесключевое хеширование и формирование хеш-значений переменной и фиксированной длины;

разработано программное средство алгоритма генерации псевдослучайных чисел на основе sponge-конструкции, обеспечивающего высокий уровень безопасности;

криптостойкость разработанных легковесных криптографических алгоритмов подтверждена с использованием общих методов криптоанализа в соответствии с их архитектурными особенностями, а также линейного, алгебраического и интегрального криптоанализа в соответствии с особенностями раундовых преобразований.

Достоверность результатов исследования. Достоверность результатов исследования подтверждена проведением строгих математических исследований применительно к предложенным алгоритмам, а также

сравнением результатов вычислительных экспериментов на основе общепринятых критериев и их подтверждением численными исследованиями. Корректность работы алгоритмов оценки по расширенным криптографическим требованиям, алгоритмов генерации S-таблиц, а также предложенных алгоритмов шифрования, хеширования и генерации псевдослучайных чисел была проверена с использованием разработанных программных средств, обеспечивающих анализ их скорости и объёма требуемой памяти.

Научная и практическая значимость результатов исследования. Научной значимостью результатов исследования являются метод генерации нелинейных преобразований, а также метод генерации раундовых преобразований для sponge-конструкции и разработанные на его основе легковесные криптографические алгоритмы.

Практическая значимость полученных в ходе исследования результатов заключается в том, что выбранные для оценки нелинейных преобразований расширенные криптографические требования могут быть использованы в качестве подходящего метода отбора алгоритмов в проводимых в Республике Узбекистан конкурсах, а раундовые преобразования с высокой стойкостью, быстродействием и различной длиной состояний могут быть использованы для построения новых легковесных криптографических алгоритмов.

Внедрение результатов исследования. На основе научных результатов, полученных в исследовательской работе по теме методов и алгоритмов криптографической защиты информации в системах Интернета вещей:

программные средства лёгковесных криптографических алгоритмов, включающих нелинейные преобразования, оценённые на основе расширенных общих криптографических требований с целью анализа существующих лёгковесных криптографических алгоритмов с точки зрения безопасности, были внедрены в рабочей среде Юго-Западного филиала АК «Узбектелеком» для криптографической защиты информации (справка Министерства Цифровых технологий Республики Узбекистан № 33-8/6636 от 17 сентября 2025 г.). В результате научного исследования алгоритм AEAD_P320, обеспечивающий конфиденциальность и целостность данных, показал самую высокую скорость среди остальных алгоритмов (в среднем 345.62 МБ/с), что на 1.02 раза выше скорости алгоритма AEAD_P384.

программные средства лёгковесных криптографических алгоритмов, включающих S-таблицы, сформированные с использованием усовершенствованного метода генерации на основе комбинированного применения расширенных синусоидальных и треугольных функций для получения нелинейных преобразований различных размеров с высокими показателями безопасности и аппаратной реализации, были внедрены в тестовой лаборатории ГУП «Центр кибербезопасность» для защиты данных (справка Министерства Цифровых технологий Республики Узбекистан, №33-8/6636 от 17 сентября 2025 г.). В результате научного исследования программное средство генератора псевдослучайных чисел обеспечило

генерацию требуемых псевдослучайных значений для криптографических алгоритмов со средней скоростью 53.932 МБ/с.

программные средства, разработанные на основе легковесных криптографических алгоритмов, обеспечивающих конфиденциальность и целостность данных, поддерживающих ключи и блоки различной длины и пригодных для реализации в устройствах Интернета вещей, были внедрены в деятельности территориального отделения инспекции «Узкомназорат» Самаркандской области для защиты информации на устройствах с ограниченными ресурсами (справка Министерства Цифровых технологий Республики Узбекистан, №33-8/6636 от 17 сентября 2025 г.). В результате научного исследования алгоритм AEAD_P320, обеспечивающий конфиденциальность и целостность данных, требовал в среднем 17.31 Кбайт ROM и 0.90 Кбайт RAM, что показало возможность его эффективной реализации даже на 32-битных микроконтроллерах. При этом все алгоритмы занимали не более 3% памяти ROM и 2% памяти RAM микроконтроллера.

программные средства, разработанные на основе лёгковесного криптографического алгоритма хеш-функции, обеспечивающего целостность данных и аутентификацию источника, поддерживающего генерацию хеш-значений переменной и фиксированной длины и реализуемого в устройствах Интернета вещей, внедрены в испытательной лаборатории ООО «UNICON.UZ – Центр научно-технических и маркетинговых исследований» для хеширования данных различной длины на плате Arduino Mega (справка Министерства Цифровых технологий Республики Узбекистан, № 33-8/6636 от 17 сентября 2025 г.). В результате научного исследования все алгоритмы при хешировании 512 байт данных требовали до 3% памяти ROM и до 5% памяти RAM микроконтроллера, обеспечивая выполнение операции за 0.2 секунды при энергопотреблении 20.5 мЖ.

программное средство, разработанное на основе лёгковесного криптографического алгоритма, обеспечивающего генерацию псевдослучайных последовательностей достаточной длины из единственного входного значения, реализуемого в устройствах Интернета вещей и обеспечивающего высокий уровень безопасности, внедрено в ООО «Intsoft-servis» для генерации псевдослучайных значений различной длины на плате Arduino Leonardo (справка Министерства Цифровых технологий Республики Узбекистан, №33-8/6636, от 17 сентября 2025 г.). В результате научного исследования алгоритм генерации псевдослучайных чисел на 8-битном микроконтроллере занимал 34% памяти ROM и 21% памяти RAM, обеспечивая генерацию 256 байт данных за 0.04 секунды при энергопотреблении 2.42 мЖ.

программные средства, разработанные на основе лёгковесных криптографических алгоритмов, оценённых с использованием общих методов криптоанализа, а также линейных, алгебраических и интегральных методов для определения криптостойкости архитектуры и раундовых преобразований, внедрены в испытательной лаборатории ООО «UNICON.UZ – Центр научно-технических и маркетинговых исследований» (справка Министерства

Цифровых технологий Республики Узбекистан, №33-8/6636, от 17 сентября 2025 г.). В результате научного исследования предложенные алгоритмы продемонстрировали устойчивость к линейному, алгебраическому и интегральному криптоанализу и обеспечили возможность реализации на 8-битных микроконтроллерах с минимальными требованиями к объёму памяти.

Апробация результатов исследования. Результаты данного исследования обсуждались на 3 международных и 8 республиканских научно-практических конференциях.

Опубликованность результатов исследования. По теме диссертации опубликовано 30 научных работ, в том числе 15 статей в научных изданиях, рекомендованных ВАК Республики Узбекистан для публикации основных научных результатов диссертаций, из них 6 статей опубликованы в зарубежных и 9 статей в республиканских журналах, а также созданы 4 программных средства для ЭВМ, на которые получены регистрационные удостоверения.

Структура и объем диссертации. Диссертация состоит из введения, пяти глав, заключения, списка литературы и приложений. Объём диссертации составляет 174 страницы.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснованы актуальность и востребованность темы диссертации, сформулированы цели и задачи, выявлены объекты и предметы исследований, определено соответствие исследования приоритетным направлениям развития науки и технологий Республики Узбекистан, изложены научная новизна и практические результаты исследований, обоснована достоверность полученных результатов, раскрыты теоретическая и практическая значимость полученных результатов, приведены внедрения в практику результатов исследований, сведения по опубликованным работам и структуре диссертации.

В первой главе диссертации **«Проблемы криптографической защиты информации в системах Интернета вещей»** описываются характеристики криптографических алгоритмов, используемых в системах Интернета вещей, результаты анализа легковесных криптографических алгоритмов и результаты оценки нелинейных преобразований на расширенных общих криптографических требований, используемых в распространенных легковесных криптографических алгоритмах.

Безопасность играет важную роль в сценарии Интернета вещей. При этом вопросы безопасности применяются на разных уровнях, от технологических проблем до более высоких, таких как, обеспечения конфиденциальности и доверия в умные игрушках. Проблемы безопасности возникают из-за природы умных объектов и стандартных протоколов. Для организации среды Интернета вещей были предложены различные архитектуры, среди которых особое значение имеет трёхслойная, состоящая из 1) прикладного уровня (уровень приложений), где выполняются приложения и сервисные задачи, 2)

сетевого/ передающего уровня (уровень сети/ передачи) и 3) уровня сбора данных/ граничного уровня (уровень восприятия/ граничного уровня), связанного с граничными точками (датчиками). Криптографические алгоритмы играют важную роль в обеспечении конфиденциальности, целостности, аутентификации источника информации и генерации псевдослучайных чисел на граничном и сетевом уровнях этой архитектуры.

Поскольку устройства Интернета вещей, как правило, обладают ограниченными энергетическими ресурсами и низкой вычислительной мощностью, важно эффективно использовать эти ресурсы (таблица 1). В частности, это следует учитывать при использовании средств безопасности и средств криптографической защиты. Результаты проведенных исследований показывают, что существующие традиционные криптографические алгоритмы не подходят для устройств Интернета вещей. Это создает необходимость разработки криптографических алгоритмов, подходящих для устройств с ограниченными энергетическими ресурсами и низкой вычислительной мощностью.

Таблица 1

Классы устройств с ограниченными возможностями согласно RFC7228 (КБ = 1024 байта, Оперативная память - ОЗУ, Постоянное запоминающее устройство - ПЗУ)

Имя	Емкость данных (ОЗУ)	Размер кода (ПЗУ, флэш-память)
Класс 0, C0	≪10 КБ	≪100 КБ
Класс 1, C1	~10 КБ	~100 КБ
Класс 2, C2	~50 КБ	~250 КБ

Криптографические алгоритмы, разработанные для таких устройств, характеризуются использованием «легковесных» качеств, так как они требует низкого энергопотребления и низкой вычислительной мощности для реализации при сохранении уровня безопасности.

Для устройств Интернета вещей было разработано множество криптографических алгоритмов, некоторые из них были приняты в качестве национальных или международных стандартов по результатам конкурсов. К ним относятся проект eSTREAM, организованный в 2004–2008 годах для отбора потоковых шифров для аппаратной и программной реализации, проект CAESAR, реализуемый Международным обществом криптографических исследований в 2012–2019 годах для отбора алгоритмов аутентифицированного шифрования с ассоциированными данными (AEAD), назначенных для использования в различных средах, конкурс NIST LWC проведенный Национальным институтом стандартов и технологий (NIST) в 2015-2023годах, проект CRYPTREC, созданный для оценки и мониторинга безопасности криптографических механизмов, используемых в японских системах электронного правительства, а также стандарт ISO/IEC 29192 (Information technology - Security techniques - Lightweight cryptography).

Легковесные криптографические алгоритмы, представленные в перечисленных выше конкурсах, проектах и стандартах, были проанализированы по таким характеристикам, как их конструктивная основа,

параметры, результаты аппаратно-программной реализации и результаты оценки криптоустойчивости с использованием различных методов криптоанализа. Анализ проводился с разделением алгоритмов на группы: шифрование, шифрование типа AEAD, коды аутентификации сообщений (Message Authentication Code, MAC), хеш-функции. В частности, в таблице 2 представлены легковесные алгоритмы шифрования типа AEAD и их характеристики. Результаты анализа показали, что существующие легковесные криптографические алгоритмы имеют недостатки, связанные с их аппаратно-программной реализацией и устойчивостью к методам криптоанализа, в частности к атакам по побочным каналам (side-channel attacks).

Во всех симметричных криптографических алгоритмах нелинейные преобразования играют важную роль в обеспечении устойчивости. Поэтому оценка нелинейных преобразований по общим криптографическим требованиям перед их использованием позволяет обеспечить их стойкость к методам криптоанализа.

Таблица 2

Легковесные алгоритмы шифрования AEAD

Имя	Тип	Базовое преобразование	Статус (бит)	Ключ (бит)	Скорость/длина блока (бит)	Тег (бит)	Безопас-ность (бит)
Ascon	Sponge	**Ascop-p**	**320**	**128**	**64**	**128**	**128**
		Ascon-p	320	128	128	128	128
Elephant	Sponge	**Spongent**	**160**	**128**	**160**	**64**	**112**
		Spongent	176	128	176	64	127
		Keccak	200	128	176	128	127
GIFT-COFB	Блочный	**GIFT-128**	**192**	**128**	**128**	**128**	**128**
Grain-128AEAD	Поточный	**Grain-128a**	**256**	**128**	**1**	**64**	**128**
ISAP	Sponge	Keccak	400	128	144	128	128
		Ascop-p	**320**	**128**	**64**	**128**	**128**
		Keccak	400	128	144	128	128
		Ascop-p	320	128	64	128	128
PHOTON-Beetle	Sponge	**ФОТОН256**	**256**	**128**	**128**	**256**	**121**
		ФОТОН256	256	128	32	256	128
Romulus	Блочный	**Skinny-128-384**	**384**	**128**	**128**	**128**	**128**
		Skinny-128-384	384	128	128	128	128
		Skinny-128-384	384	128	128	128	128
SPARKLE	Sponge	**SPARKLE**	**256**	**128**	**128**	**128**	**120**
		SPARKLE	384	128	256	128	120
		SPARKLE	384	192	192	192	184
		SPARKLE	512	256	256	256	248
TinyJambu	Sponge	**TinyJambu**	**128**	**128**	**32**	**64**	**120**
Xoodyak	Sponge	**Xoodoo**	**384**	**128**	**352**	**128**	**128**
AES-GCM	Блочный	**AES**	**128**	**128, 256**	**128**	96, 104, 112, 120, **128**	64 **128**

Примечание: Параметры, выделенные жирным шрифтом, — это основные варианты, предоставленные авторами.

Общие криптографические требования в основном предназначены для оценки традиционных нелинейных преобразований, однако при оценке

нелинейных преобразований в легковесных криптографических алгоритмах возникает необходимость введения дополнительных критериев. Поэтому при оценке нелинейных преобразований в легковесных криптографических алгоритмах были использованы расширенные общие криптографические требования, включающие следующие критерии:

- общие критерии: сбалансированность и регулярность, строгий критерий лавинного смещения (Strict Avalanche Criterion, SAC), критерий независимости битов (Bit Independence Criterion, BIC), фиксированная точка (Fixed point, FP) и противоположная фиксированная точка (Opposed fixed point, OFP);
- критерии стойкости к линейному криптоанализу: нелинейность (Nonlinearity, NL), корреляционный иммунитет (Correlation immunity, CI), вероятность линейной аппроксимации (Linear Approximation Probability, LP), число линейной ветвления (Linear branch number, LBN);
- критерии устойчивости к дифференциальному криптоанализу: критерии распространения (Propagation Criteria, PC), дифференциальная аппроксимационная вероятность (Differential Approximation Probability, DP), дифференциальное число ветвления (Differential branch number, DBN);
- критерии устойчивости к алгебраическому криптоанализу: уровень алгебраического иммунитета (Algebraic immunity, AI) и количество требуемых уравнений (КУ);
- критерии, указывающие на устойчивость к атаке с использованием дифференциального анализа мощности (Differential power analysis, DPA): порядок прозрачности (Transparency order, TO), отношение сигнал/шум (Signal-to-Noise Ratio, SNR), дисперсия коэффициента путаницы (Confusion coefficient variance, CCV);
- критерии эффективности аппаратной реализации: количество логических элементов (ЛЭ).

Результаты оценки S-таблиц различных размеров по выбранным критериям представлены в таблице 3.

Полученные результаты анализа показывают, что в качестве нелинейных преобразований в легковесных криптографических симметричных алгоритмах используются S-таблицы малого размера, которые не обладают высокой стойкостью к ряду атак криптоанализа, в частности атакам по сторонним каналам, и не обеспечивают высокой эффективности при аппаратной реализации.

Во второй главе диссертации **«Криптостойкие преобразования для легковесных симметричных криптосистем»** представлены сведения о значении конструкции sponge при построении легковесных криптографических алгоритмов, метод и алгоритм построения нелинейных преобразований различной длины для легковесных криптографических алгоритмов, процедура построения раундовых преобразований для различной длины состояний и результаты анализа полученных с их помощью.

В частности, в разделе 2.1 обсуждается важность sponge-конструкции для построения легковесных криптографических алгоритмов. При построении

легковесных криптографических алгоритмов sponge-конструкция широко используется, как показано в таблице 2.

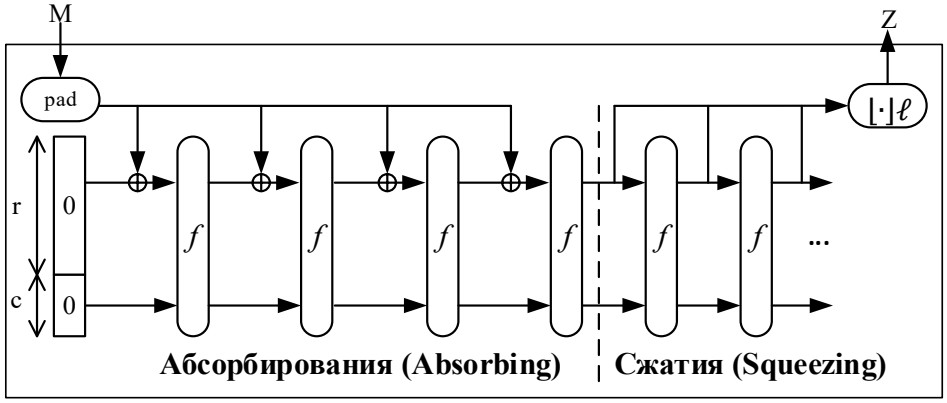
Таблица 3

Результаты оценки S-таблиц различных размеров по расширенным общим криптографическим требованиям

№	Источник	Общий					Линейный				Дифферен.			Алг.	DPA			Реа.
		B +	FP ↓	OFP ↓	SAC (=0.5)	BIC-SAC (=0.5)	NL ↑	LP ↓	CI ↑	LBN ↑	DP ↓	PC ↑	DBN ↑	AI, КУ ↑	TO ↓	CCV ↑	SNR ↓	ЛЭ ↓
4x4 S таблицы																		
1.	Present	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
2.	FEATHER	+	1	0	0.562	0.531	4	0.25	0,0,0,0	2	0.375	0	2	2, 21	3.533	0.457	2.398	23
3.	ARSHAD (8)	+	0	4	0.500	0.520	4	0.25	0,0,0,0	2	0.375	0	2	2, 21	3.666	0.382	2.259	20
4.	IVLBC	+	4	0	0.546	0.531	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.666	0.257	2.806	8
5.	DBST (1)	+	1	0	0.640	0.468	4	0.25	0,0,1,1	2	0.250	0	2	2, 21	3.600	0.307	2.685	14
6.	ELEPHANT	+	0	1	0.656	0.520	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.266	0.457	2.398	15
7.	GIFT	+	0	1	0.625	0.541	4	0.25	0,0,1,1	2	0.375	0	2	2, 21	3.600	0.457	2.398	15
8.	KNOT	+	0	2	0.671	0.479	4	0.25	1,1,0,0	2	0.250	0	2	2, 21	3.333	0.607	2.187	16
9.	PYJAMASK	+	0	2	0.593	0.520	4	0.25	1,0,0,0	2	0.250	0	2	2, 21	3.466	0.607	2.187	16
10.	SATURNIN	+	1	0	0.531	0.500	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.533	0.357	2.578	16
11.	SPOOK	+	1	2	0.515	0.562	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.666	0.307	2.685	8
12.	KLEIN	+	0	0	0.593	0.500	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.466	1.207	1.691	23
13.	RECTANGLE	+	0	0	0.671	0.479	4	0.25	0,0,1,1	2	0.250	0	2	2, 21	3.400	0.607	2.187	17
14.	PRIDE	+	4	0	0.500	0.541	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.533	0.307	2.685	8
15.	CRAFT	+	4	2	0.406	0.562	4	0.25	0,0,0,0	2	0.250	0	2	2, 21	3.466	1.257	1.663	18
16.	Duong	+	0	0	0.500	0.500	4	0.25	0,0,1,0	2	0.250	0	2	2, 21	3.400	1.357	1.612	19
17.	Photon	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
18.	Magma 0	+	1	0	0.515	0.520	4	0.25	0,0,0,0	2	0.25	0	2	2, 21	3.533	0.357	2.578	21
5x5 S таблицы																		
19.	Ascon	+	0	0	0.619	0.520	8	0.25	1,1,1,1,1	3	0.250	0	3	2, 25	4.322	0.501	3.015	20
20.	PRIMATE	+	0	2	0.540	0.510	12	0.125	0,0,0,0,0	2	0.062	0	2	2, 25	4.837	0.308	3.535	27
21.	ICEPOLE	+	0	2	0.425	0.550	8	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.516	0.190	4.025	30
22.	SYCON	+	0	0	0.620	0.520	8	0.25	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	20
23.	Duong	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 25	4.580	1.275	2.085	41
24.	Thakor	+	0	1	0.540	0.507	8.4	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.596	0.347	3.408	42
25.	Irfan	+	0	0	0.540	0.525	8.8	0.25	0,0,0,0,0	2	0.250	0	2	2, 25	4.532	0.259	3.713	40
6x6 S таблицы																		
26.	Yan	+	0	2	0.503	0.754	24	0.125	1,1,1,0,0,0	2	0.062	0	2	2, 28	5.452	0.402	4.086	49
27.	Kim	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.670	0.339	4.341	44
28.	Sarkar 1	+	4	2	0.569	0.775	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 28	5.714	0.402	4.086	39
29.	Sarkar 2	+	2	0	0.565	0.764	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 28	5.595	0.342	4.328	72
30.	Bilgin	+	0	1	0.508	0.764	24	0.125	0,0,0,0,0,0	2	0.031	0	2	2, 22	5.730	0.238	4.879	73
8x9 S таблицы																		
31.	Abdurazzokov	+	0	1	0.494	0.497	105.0	0.132	0,0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.801	0.118	9.408	-
32.	AES	+	0	0	0.504	0.504	112.0	0.062	0,0,0,0,0,0,0,0,0	2	0.015	0	2	2, 39	7.860	0.111	9.599	-
33.	Kuznechik	+	0	0	0.512	0.494	106.5	0.109	0,0,0,0,0,0,0,0,0	2	0.031	0	2	3, 441	7.835	0.112	9.570	-
34.	Romulus	+	1	0	0.316	0.431	64.0	0.250	0,0,0,0,0,0,0,0,0	2	0.250	0	2	2, 34	7.174	0.340	6.312	-
35.	Manzoor	+	2	1	0.503	0.504	110	0.132	0,0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.818	0.098	9.976	-
36.	Alqahtani	+	1	2	0.505	0.502	102.7	0.132	0,0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.808	0.124	9.251	-

Конструкция sponge представляет собой простую итеративную (пошаговую) конструкцию, используемую для генерации выходных данных любой длины из входного сообщения переменной длины, которое является сообщением фиксированной длины и основывается на функции f преобразования или перестановки над битамы b фиксированной длины. Здесь

b – называется общим размером состояния (рис. 1). Конструкция Sponge работает с побитовым состоянием $b = r + c$, где: r - объём данных (вход/выход) (битрейт), c - ёмкость, скрытая часть, обеспечивающая безопасность.



Sponge

Рисунок 1. Конструкция Sponge

Конструкция Sponge функционирует в два этапа:

1. Стадия абсорбирования: входящее сообщение разделяется на блоки r битов и дополняется специальным методом до тех пор, пока его длина не станет кратной длине блока. Каждый блок подвергается операции XOR с первым r битом состояния. Затем для принятого в качестве входного значения состояния применяется функция f. После вставки всех блоков выполняется этап сжатия.

2. Стадия сжатия: первый r бит состояния принимается в качестве выходного блока. После каждого выходного блока f функция применяется снова. Пользователь может выбрать любую длину выходного блока. Последний c биты состояния никогда не подвергаются непосредственному воздействию входных блоков и никогда не выводятся на этапе сжатия.

Правило заполнения данных. Для конструкции sponge используются два метода заполнения данными: простой и многочастотной. *Простое заполнение*, обозначается как $pad10^*$, и добавляется один единичный бит, за которым следует минимальное количество нулевых битов, необходимое для того, чтобы длина результата стала кратной длине блока. *Многочастотное наполнение*, отмечено как $pad10^*1$, добавляется один единичный бит, затем добавляется минимальное количество нулевых битов, необходимое для того, чтобы результат стал кратным длине блока, затем добавляется еще один единичный бит.

Конструкция sponge относительно общих атак обеспечивает c/2 уровень безопасности. В частности, обеспечивается уровень безопасности от коллизий, нахождения второго прообраза, различения, подделки и атаки расширения длины - на уровне $2^{c/2}$; от нахождения прообраза - на уровне $\min(2^n, 2^c)$; от восстановления ключа - на уровне $\min(2^{c/2}, 2^c, 2^k)$; а для режимов с ключом для атаки «встреча посередине» - на уровне $\min(2^{c/2}, 2^{k/2})$ или в бесключевых режимах для нахождения прообраза - на уровне $\min(2^n, 2^{c/2})$.

Базовые атаки зависят от возможности проведения различения, и если

раундовое преобразование является слабым, граница $2^{c/2}$ может быть нарушена. Длина ключа (k) влияет только на восстановление ключа и не оказывает воздействия на атаки, направленные на столкновения, подделку или различение (поэтому величина 2^k здесь не применяется, если только восстановление ключа не выполняется раньше). Герметичная sponge-конструкция позволяет проектировать преобразование f с высокой диффузией, нелинейностью и без структурных особенностей, которые могли бы облегчить различение, что обеспечивает соответствие безопасности установленным общим пределам.

В разделе 2.2 этой главы обсуждается построение нелинейных функций для раундовых преобразований в sponge-конструкции. Сначала был усовершенствован метод построения S-таблиц на основе хаотических преобразований и предложен соответствующий алгоритм.

Хаотические системы также называются нелинейными динамическими системами, поскольку между входными и выходными данными нет прямой связи. На практике для построения и определения уровня хаоса в системах используется ряд методов, включая бифуркационную диаграмму и показатель Ляпунова (ПЛ).

Например, так называемое логистическое преобразование, или хаотическое преобразование, выражается следующим образом:

$$x_{n+1} = ax_n(1 - x_n),$$

где, a - управляющий параметр, x_n - значение, генерируемое n раз.

В настоящей работе метод, основанный на хаотических преобразованиях, усовершенствован путем использования расширенных функций синуса (Enhanced Sine map) и треугольная (Enhanced Tent map):

$$x_{i+1} = f(x_i, a) = \begin{cases} \sin(a\pi\sin(\pi x_i)) + \sin(\pi a x_i) & x_i < 0.5 \\ \sin(a\pi\sin(\pi x_i)) + \sin(\pi a(1 - x_i)) & x_i \geq 0.5 \end{cases}$$

где a - управляющий параметр, а $a \in (0, +\infty)$ - подходящий. В этом уравнении x_i значения амплитуды лежат в диапазоне $[-2, 2]$.

Предложенный алгоритм построения таблицы S на основе хаотического преобразования представлен на рисунке 2.

Этот алгоритм основан на проверке на соответствие предопределенным требованиям при построении таблицы S из значений, сгенерированных хаотическим преобразованием. Результаты оценки сгенерированных S-таблиц на соответствие вышеуказанным расширенным общим требованиям представлены в таблице 4.

Кроме того, путем изучения влияния аффинного преобразования на свойства S-таблиц предложен новый эффективный алгоритм генерации S-таблиц. Аффинное преобразование - математическая операция, используемая в криптографии, в частности, при разработке симметричных блочных шифров и S-таблиц, которая сочетает линейное преобразование и сложение по модулю с инвариантом. Аффинное преобразование помогает внести нелинейность и смешивание в криптографические алгоритмы.

Определение 1. $GF(2^n)$ Аффинное преобразование в конечном поле выражается как:

$$Y = A \cdot X \oplus B$$

здесь, X – обозначает входной вектор размером n бит, A – обозначает $n \times n$ матрицу с обратной матрицей в поле $GF(2)$, B – обозначает инвариантный вектор размером n бит, Y – обозначает выходной вектор размером n бит, $\oplus$ - обозначает побитовую операцию XOR.

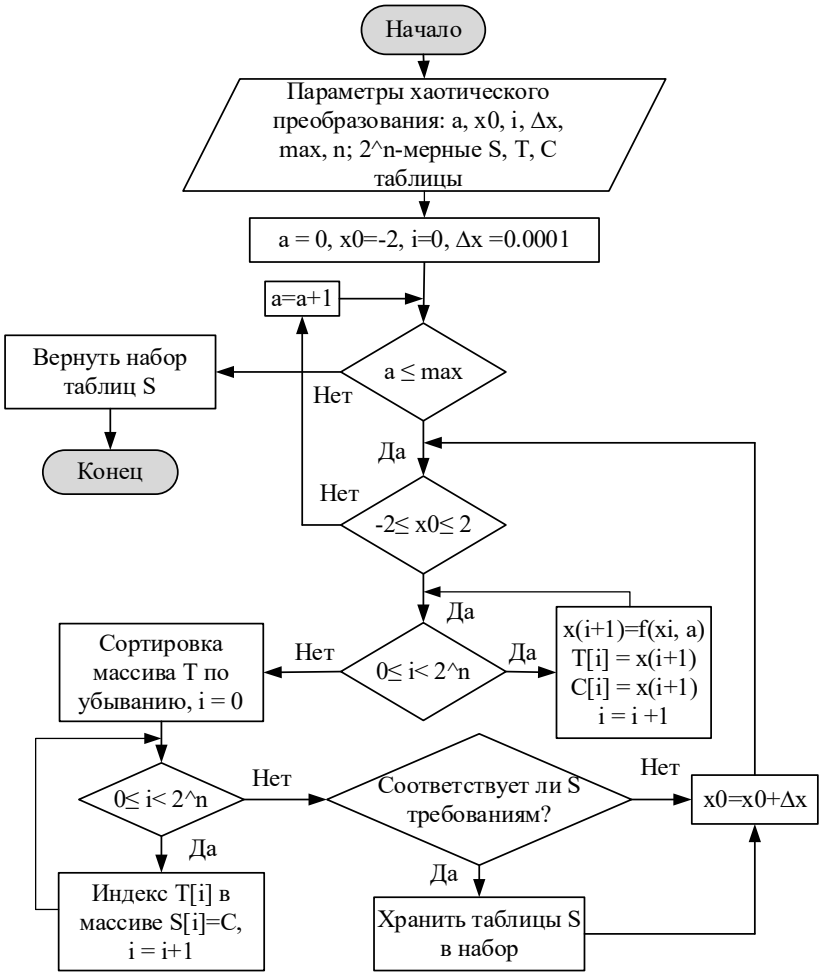


Рисунок 2. Алгоритм построения таблицы S

В целом он хорошо рассчитывается для новых расширенных криптографических требований с использованием аффинного преобразования из существующей таблицы S. Блок-схема алгоритма формирования S-таблицы представлена на рисунке 3.

Результаты оценки сгенерированных S-таблиц на соответствие вышеуказанным расширенным общим требованиям представлено в таблице 5. В таблице 8 перечислены новые S-таблицы и характеристики, которые делают их лучше существующих. Выделенные ячейки в столбце «Название S-таблицы» указывают на S-таблицы, обладающие несколькими характеристиками, превосходящими существующие.

В предлагаемых раундовых преобразованиях для использования в качестве нелинейной операции выбраны S-таблицы, приведённые ниже:

S_Box1 (4×4) = (6, 10, 12, 1, 3, 15, 5, 2, 9, 4, 0, 7, 14, 8, 11, 13);

S_Box1 (5×5) = (6, 9, 27, 22, 17, 30, 13, 0, 25, 14, 5, 16, 31, 8, 2, 23, 19, 24, 10, 3, 4, 15, 28, 21, 20, 7, 12, 29, 18, 1, 11, 26);

S_Box21 (6×6) = (40, 13, 24, 53, 21, 34, 1, 62, 59, 18, 9, 44, 36, 29, 50, 7, 33, 11, 30, 57, 47, 23, 54, 3, 48, 14, 38, 17, 42, 4, 26, 61, 63, 22, 6, 39, 52, 10, 45, 27, 19, 43, 12, 56, 28, 49, 35, 2, 0, 46, 51, 16, 25, 32, 8, 60, 55, 20, 15, 37, 31, 41, 5, 58).

Таблица 4

Результаты оценки сгенерированных S-таблиц на предмет соответствия требованиям безопасности

Таблица S	Общий					Линейный				Дифферен.			Алг.	DPA			Реа.
	B+	FP↓	OFP↓	SAC (=0.5)	BIC-SAC (=0.5)	NL↑	LP↓	CI↑	LBN↑	DP↓	PC↑	DBN ↑	AI, КУ↑	TO↓	CCV↑	SNR↓	ЛЭ↓
4x4 S таблицы																	
S_Box1	+	0	0	0.500	0.500	4	0,25	0,0,0,0	2	0.25	0	2	2, 21	3.733	1.207	1.691	19
S_Box2	+	0	0	0.500	0.500	4	0,25	0,0,0,0	2	0.25	0	2	2, 21	3.533	1.182	1.705	19
S_Box3	+	0	0	0.500	0.500	4	0,25	0,0,0,0	2	0.25	0	2	2, 21	3.533	1.382	1.600	22
S_Box4	+	0	0	0.500	0.500	4	0,25	0,0,0,0	2	0.25	0	2	2, 21	3.666	1.207	1.691	21
5x5 S таблицы																	
S_Box1	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 24	4.645	1.194	2.144	43
S_Box2	+	0	0	0.500	0.500	10	0.25	0,0,0,0,0	2	0.187	0	2	2, 24	4.661	1.293	2.072	42
S_Box3	+	0	0	0.575	0.532	9.6	0.25	0,0,0,0,0	2	0.25	0	3	2, 24	4.645	0.347	3.408	41
6x6 S таблицы																	
S_Box1	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.599	0.339	4.341	44
8x8 S таблицы																	
S_Box1	+	0	0	0.494	0.507	106.5	0.125	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.799	0.126	9.208	-
S_Box2	+	0	0	0.501	0.502	107	0.148	0,0,0,0,0,0,0,0	2	0.039	0	2	3, 441	7.808	0.119	9.384	-

В разделе 2.3 настоящей главы были разработаны раундовые преобразования с длиной состояния 256, 320 и 384 бит ($S = S_r \parallel S_c$) (обозначенные условными названиями P256, P320 и P384 соответственно), которые в общем случае выражаются следующим образом:

$$p = p_L \cdot p_S \cdot p_C$$

Здесь, p_L – обозначает линейный этап, p_S – нелинейный этап и p_C – этап добавления раундовых инвариантов, которые подробно описаны ниже.

Линейный этап p_L. Линейный этап состоит из циклического сдвига и операции XOR над 64-битными словами, выполняя не только внутрисловное, но и межсловное перемешивание. Эти выражения используют следующее равенство для случаев 256 бит ($i \in [0,3]$ и $n = 4$), 320 бит ($i \in [0,4]$ и $n = 5$) и 384 бит ($i \in [0,5]$ и $n = 6$):

$$x'_i \leftarrow x_i \oplus (x_i \ggg C1_i) \oplus (x_i \ggg C2_i) \oplus (x_{(i+1) mod\, n} \ggg 11)$$

здесь, $C1 = \{7,15,2,18,9,17\}$ и $C2 = \{36,52,25,44,60,35\}$ равны. Значения внутрисловных и межсловных циклических сдвигов были выбраны для максимизации потенциала перемешивания и достижения низкой стоимости реализации. Количество ветвей этого линейного преобразования также равно 5, достигая максимального индекса перемешивания после 3-го раунда.

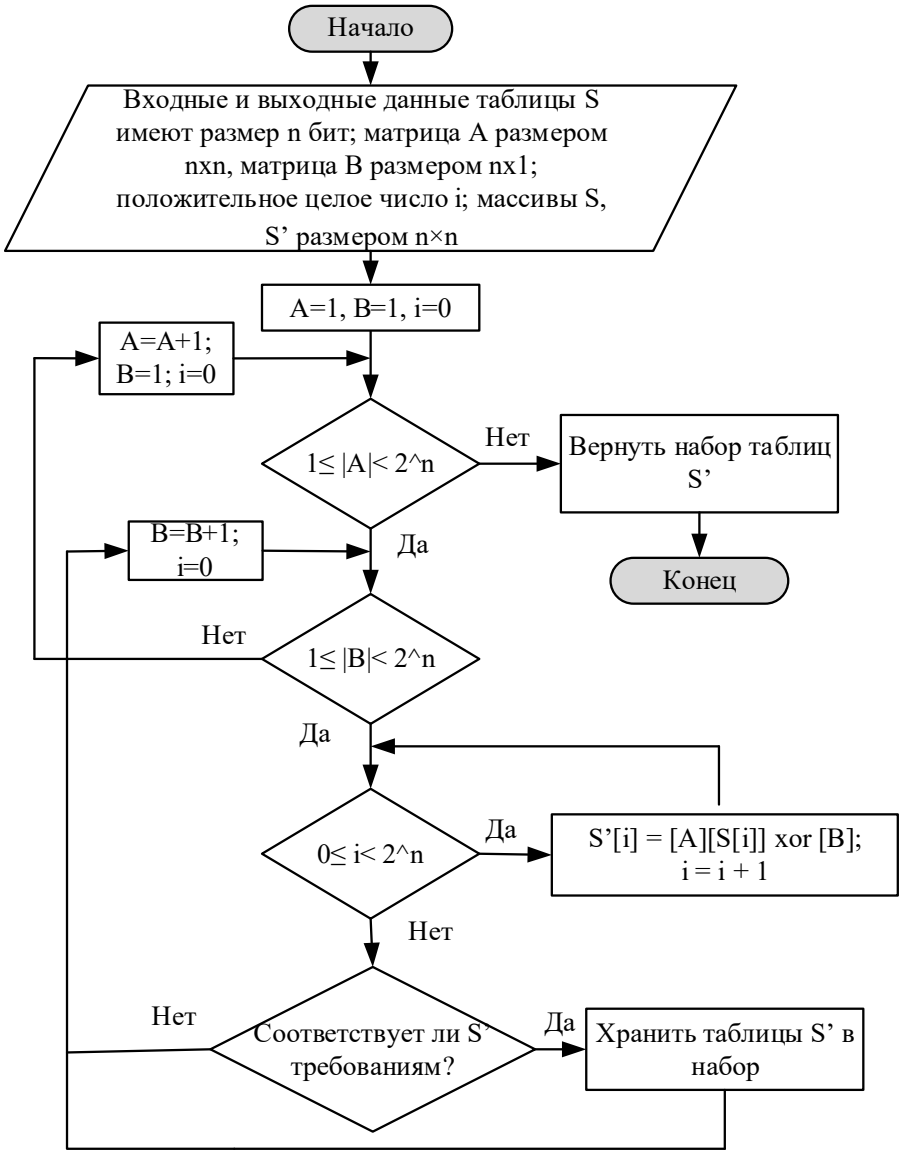


Рисунок 3. Блок-схема алгоритма генерации новой таблицы S с использованием аффинного преобразования из таблицы S

Нелинейный этап p_S. Этот шаг является важным шагом в преобразовании, в котором для 256-битного случая используется таблица S размером 4×4, а для 320-битного случая таблица S размером 5×5, а для 384-битного случая таблица S размером 6×6. Эти таблицы S приведены выше.

Добавление констант раунда p_C. Для генерации раундовых константов для раундового преобразования использовался подход на основе регистра сдвига с линейной обратной связью. Для этого был использован примитивный многочлен $p(x) = x^8 + x^6 + x^5 + x^4 + 1$. Кроме того, учитывая требование, чтобы генерируемые значения имели вес Хемминга не менее 4, необходимо инициализировать их начальными значениями (seeds), такими как 0x0d (13), 0x0e (14), 0x0f (15), 0x15 (21) и 0x3b (59).

Третья глава диссертации **«Легковесные алгоритмы симметричного аутентифицированного шифрования»** рассматривает вопрос создания раундовых преобразований для конструкции sponge с 320- и 384-битными состояниями и построения на их основе легковесных алгоритмов

симметричного блочного аутентифицированного шифрования.

Таблица 5

Результаты создания новых таблиц на основе существующих таблиц S

Название таблицы S	Общий					Линейный				Дифферен.			Алг.	DPA			Реа.
	B+	FP↓	OFP↓	SAC (=0.5)	BIC-SAC (=0.5)	NL↑	LP↓	CI↑	LBN ↑	DP↓	PC↑	DBN ↑	AI, КУ↑	TO↓	CCV↑	SNR↓	ЛЭ↓
4x4 S таблицы																	
Present	+	0	1	0.625	0.562	4	0.25	0,0,0,1	2	0.250	0	3	2, 21	3.600	0.657	2.128	16
S_Box1	+	0	0	0.625	0.562	4	0.25	0,1,0,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	14
S_Box2	+	0	0	0.625	0.562	4	0.25	0,0,1,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	15
S_Box3	+	0	0	0.625	0.562	4	0.25	0,0,1,0	2	0.250	0	3	2, 21	3.533	0.657	2.128	14
5x5 S таблицы																	
Ascon	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.322	0.501	3.015	20
S_Box1	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box2	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box8	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box14	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
S_Box18	+	0	0	0.619	0.520	8	0.250	1,1,1,1,1	3	0.250	0	3	2, 25	4.258	0.501	3.015	19
6x6 S таблицы																	
S_Box0	+	2	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.599	0.339	4.341	44
S_Box21	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.539	0.447	3.929	43
S_Box23	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.583	0.423	4.010	43
S_Box26	+	0	0	0.576	0.756	24	0.125	1,1,1,1,1,1	3	0.062	0	3	2, 22	5.583	0.542	3.646	44

Предлагаемые в этой главе, алгоритмы шифрования AEAD основаны на преобразованиях P320 и P384, а их общие параметры приведены в таблице 6. Здесь, (k) длина ключа, (r) длина блока, a и b внутренние значения раунда. Также, случайное слово (Nonce, N), (AD) A данные ассоциации переменной длины, T тег аутентификации и вектор инициализации (вектор инициализации, IV). Исходя из этого, функция шифрования может быть определена как $E_{k,r,a,b}(K,N,A,P)=(C,T)$, а соответствующая функция расшифрования - как $D_{k,r,a,b}(K,N,A,C,T)\in\{P,\perp\}$. Здесь шифротекст C и расшифрование возвращают открытый текст P, если тег аутентификации верны, в противном случае ошибку $\perp$.

Таблица 6

Параметры предлагаемых алгоритмов AEAD

Имя	Алгоритмы	k, бит	nonce, бит	тег, бит	b, бит	c, бит	IV, бит	A, бит	r, бит	Количество раундов		Уровень безопас-ности
										a	b	
AEAD-P320	$E, D_{128,64,12,6}$	128	128	128	320	256	64	$\{0,1\}^*$	64	12	6	128
AEAD-P384	$E, D_{128,128,14,8}$	128	128	128	384	256	128	$\{0,1\}^*$	128	14	8	128
AEAD-P384a	$E, D_{192,128,14,8}$	192	128	128	384	256	64	$\{0,1\}^*$	128	14	8	128

Все шифры AEAD-P320, AEAD-P384 и AEAD-384a, как правило, работают на основе алгоритма 1. Изменяя параметры в этом алгоритме, можно легко разработать режимы шифрования AEAD-P320, AEAD-P384 и AEAD-384a.

Начальное состояние во всех вариантах алгоритма (320 или 384 бита) k битное ключ K формируется с использованием 128 битного nonce N и следующего 64-битного параметра алгоритма (для AEAD-P320) или 128-битного вектора инициализации:

$$IV_{k,r,a,b} \leftarrow k \parallel r \parallel a \parallel b \parallel 10^*1$$
$$= \begin{cases} 80400c0680000001 \quad \text{для } AEAD-P320 \\ 80800e088000000000000000000000001 \quad \text{для } AEAD-P384 \\ c0800e0880000001 \quad \text{для } AEAD-P384a \end{cases}$$

В этом случае начальное состояние равно $S \longleftarrow IV_{k,r,a,b} \parallel K \parallel N$.

Алгоритм 1. Процедуры для шифров AEAD-P320, AEAD-P384 и AEAD-384a

Аутентифицированное шифрования	**Проверенная расшифровка**
Введение: открытый текст $P \in \{0,1\}^*$, ключ, $K \in \{0,1\}^k$ Nonce $N \in \{0,1\}^{128}$ связяанная информация $A \in \{0,1\}^*$ **Выход:** зашифрованный текст $C \in \{0,1\}^{\lvert P\rvert}$, тег $T \in \{0,1\}^{128}$	**Введение:** открытый текст $P \in \{0,1\}^*$, ключ $K \in \{0,1\}^k$ Nonce $N \in \{0,1\}^{128}$ связанная информация, $A \in \{0,1\}^*$ тег $T \in \{0,1\}^{128}$ **Выход:** открытый текст $P \in \{0,1\}^{\lvert C\rvert}$ или $\perp$

Инициализация
$S \leftarrow IV_{k,r,a,b} \parallel K \parallel N$
$S \longleftarrow p^a(S) \oplus (0^{b-k} \parallel K)$
Обработка связанной информации
if $\lvert A\rvert > 0$ **then**
$A_1 \dots A_s \leftarrow A \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, s$ **do**
$S \leftarrow p^b(S_r \oplus A_i \parallel S_c)$
$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
Обработка данных
$P_1 \dots P_t \leftarrow P \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, t-1$ **do**
$S_r \leftarrow S_r \oplus P_i$
$C_i \leftarrow S_r$
$S \longleftarrow p^b(S)$
$S_r \leftarrow S_r \oplus P_t$
$\hat{C}_t \leftarrow \lfloor S_r \rfloor_{\lvert P\rvert \bmod r}$
Завершение
$S \longleftarrow p^a(S \oplus (0^r \parallel K \parallel 0^{c-k})$
for $i = 1, \dots, d = \lvert T\rvert / r$ **do**
$S \longleftarrow p^a(S)$
$T_i \longleftarrow S_r$
return $C_1 \parallel \cdots \parallel C_{t-1} \parallel \hat{C}_t, T$
	Инициализация
	$S \leftarrow IV_{k,r,a,b} \parallel K \parallel N$
	$S \longleftarrow p^a(S) \oplus (0^{b-k} \parallel K)$
	Обработка связанной информации
	if $\lvert A\rvert > 0$ **then**
	$A_1 \dots A_s \leftarrow A \parallel 1 \parallel 0^* \parallel 1$
	for $i = 1, \dots, s$ **do**
	$S \leftarrow p^b(S_r \oplus A_i \parallel S_c)$
	$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
	Обработка шифротекста
	$C_1 \dots C_{t-1} \hat{C}_t \leftarrow C, 0 \le \lvert \hat{C}_t \rvert < r$
	for $i = 1, \dots, t-1$ **do**
	$P_i \leftarrow S_r \oplus C_i$
	$S \leftarrow C_i \parallel S_c$
	$S \longleftarrow p^b(S)$
	$\hat{P}_t \leftarrow \lfloor S_r \rfloor_{\lvert \hat{C}_t \rvert} \oplus \hat{C}_t$
	$S_r \leftarrow S_r \oplus (\hat{P}_t \parallel 1 \parallel 0^* \parallel 1)$
	Завершение
	$S \longleftarrow p^a(S \oplus (0^r \parallel K \parallel 0^{c-k})$
	for $i = 1, \dots, d = \lvert T\rvert / r$ **do**
	$S \longleftarrow p^a(S), T^*{}_i \longleftarrow S_r$
	if $T = T^*$ **return** $P_1 \parallel \cdots \parallel P_{t-1} \parallel \hat{P}_t$ **else** $\perp$

В четвертой главе диссертации «**Методы и алгоритмы построения легковесной хэш-функции и генератора псевдослучайных чисел**» рассматриваются методы и алгоритмы генерации ключевых/бесключевых, фиксированной/переменной длины хэш-значений на основе 320- и 384-битных

раундовых преобразований, а также построения генератора псевдослучайных чисел на основе 256-битных раундовых преобразований.

Разработанные хэш-функции основаны на конструкции sponge с двумя преобразованиями длины состояния 320 и 384 бит соответственно, обновляются с помощью P320 и P384. В целом, как бесключевые, так и ключевые хэш-функции, а также значения хэш-функций фиксированной и переменной длины однозначно представлены длиной ключа k (если режим бесключевого доступа $k = 0$), длина блока (64 бита для преобразования P320 и 128 бит для преобразования P384) r, длина хэш-значения h (если оно переменной длины $h = 0$) и количество a раундов используются в качестве параметров. Исходя из этого, предлагаемые хэш-функции $X_{k,r,a,h}$ сопоставляют входные данные сообщения переменной длины M и ключ K с выходными H данными длиной$l \leq h$:

$$X_{k,r,a,h}(K, M, l) = H.$$

Для вариантов хеш-функции фиксированной длины он равен $h = 256$, а для вариантов переменной длины - $h = 0$. Соответственно, в режиме с ключом ключи равны 128 или 192, а в режиме без ключа будет равно $k = 0$.

Название и длина ключа предлагаемых алгоритмов хеширования k, длина блока r, длина хэш-значения h, количество раундов преобразования a для всех этапов алгоритма, начальный вектор IV, длина состояния в преобразованиях b, длина емкости c и уровень безопасности приведены в таблице 7. Опции, начинающиеся с буквы «K» в названии, указывают на то, что используется ключевой режим, а наличие фразы «HASH» указывает на то, что хэш-функция имеет фиксированную длину, «XOF» (Extended output function, Xof) указывает на то, что это опция, которая генерирует хэш-значение переменной длины.

Таблица 7

Параметры предлагаемых алгоритмов хеш-функций

Название алгоритма	Статус, b, бит	Емкость, c, бит	IV, бит	k, бит	h, бит	r, бит	a	Уровень безопасности, бит
KHASH-P320	320	256	64	128	256	64	12	128
KHASH-P320a	320	256	64	192	256	64	12	128
KXOF-P320	320	256	64	128	0	64	12	$min\,(128, l/2)$
KXOF-P320a	320	256	64	192	0	64	12	$min\,(128, l/2)$
KHASH-P384	384	256	128	128	256	128	14	128
KHASH-P384a	384	256	128	192	256	128	14	128
KXOF-P384	384	256	128	128	0	128	14	$min\,(128, l/2)$
KXOF-P384a	384	256	128	192	0	128	14	$min\,(128, l/2)$
HASH-P320	320	256	64	0	256	64	12	128
XOF-P320	320	256	64	0	0	64	12	$min\,(128, l/2)$
HASH-P384	384	256	128	0	256	128	14	128
XOF-P384	384	256	128	0	0	128	14	$min\,(128, l/2)$

Схема метода построения ключевых хеш-функций на основе обоих преобразований представлена на рисунке 4.

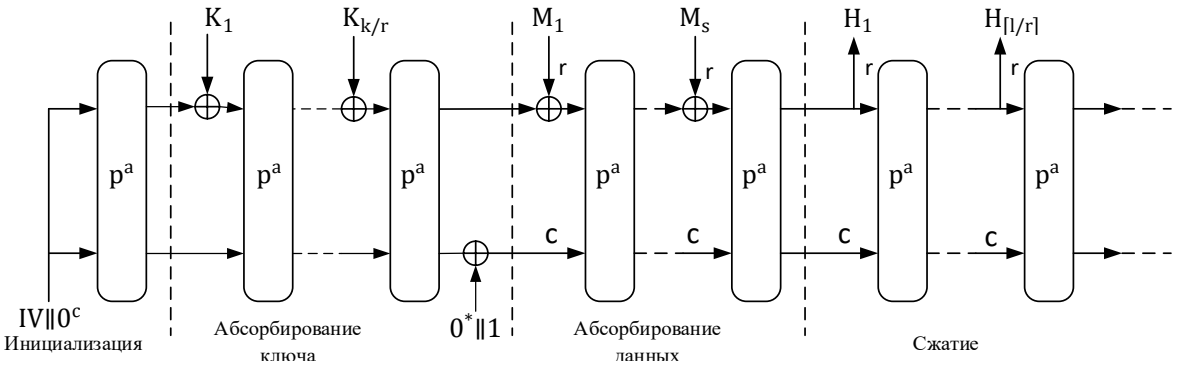


Рисунок 4. Схема метода построения хэш-функций в ключевом режиме

Все алгоритмы ключевых хэш-функций обычно работают на основе следующего алгоритма 2. Соответственно, все алгоритмы хеш-функций без ключа, как правило, работают на основе следующего алгоритма 3.

Длина ключа начального вектора IV для всех вариантов хэш-функций, основанных на преобразовании P320, составляет 64 бита, он доступен как для режима с ключом, так и для режима без ключа, рассчитывается следующим образом: $IV_{k,r,a,h} \leftarrow k \parallel r \parallel a \parallel h \parallel 10^*1$. Здесь один байт выделяется для k, r, a, а для h выделяется 2 байта.

Алгоритм 2. Процедура алгоритмов ключевой хэш-функции	**Алгоритм 3. Процедура алгоритмов бесключевой хэш-функции**
Введение: сообщение $M \in \{0,1\}^*$, ключ $K \in \{0,1\}^k$, выходной битовый размер $l = h$ или значение переменной для $h = 0$. **Выход:** хэш-значение $H \in \{0,1\}^l$	**Введение:** сообщение $M \in \{0,1\}^*$, для выходного размера бита $l = h$ или значения переменной $h = 0$. **Выход:** хэш-значение $H \in \{0,1\}^l$

Инициализация
$S \leftarrow p^a(IV_{k,r,a,h} \parallel 0^c)$
Абсорбирование ключа
$K_1 \dots K_d \leftarrow K \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, d$ do
$S \leftarrow p^a(S_r \oplus K_i \parallel S_c)$
$S \leftarrow S \oplus (0^{b-1} \parallel 1)$
Абсорбирование данных
$M_1 \dots M_s \leftarrow M \parallel 1 \parallel 0^* \parallel 1$
for $i = 1, \dots, s$ do
$S \leftarrow p^a(S_r \oplus M_i \parallel S_c)$
Сжатие
for $i = 1, \dots, t = \lceil l/r \rceil$ do
$H_i \leftarrow S_r$
$S \leftarrow p^a(S)$
return $\lfloor H_1 \parallel \cdots \parallel H_t \rfloor_l$
	Инициализация
	$S \leftarrow p^a(IV_{k,r,a,h} \parallel 0^c)$
	Абсорбирование
	$M_1 \dots M_s \leftarrow M \parallel 1 \parallel 0^* \parallel 1$
	for $i = 1, \dots, s$ do
	$S \leftarrow p^a(S_r \oplus M_i \parallel S_c)$
	Сжатие
	for $i = 1, \dots, t = \lceil l/r \rceil$ do
	$H_i \leftarrow S_r$
	$S \leftarrow p^a(S)$
	return $\lfloor H_1 \parallel \cdots \parallel H_t \rfloor_l$

Соответственно, начальные векторы для всех вариантов хэш-функции на основе преобразования P384 рассчитываются следующим образом: $IV_{k,r,a,h} \leftarrow k \parallel r \parallel a \parallel h \parallel 10^*1$. Здесь один байт выделено для k, r, a, а для h выделено 2 байта.

Также в разделе 4.3 разработан алгоритм генерации псевдослучайных чисел (ГПСЧ), основанный на преобразовании P256. Параметры,

использованные для построения ГПСЧ, перечислены в таблице 8. Алгоритм устойчив к атакам, связанным с реконструкцией состояния, и имеет 2^{128} сопротивления.

Таблица 8

Рекомендуемые параметры для ГПСЧ (в битах)

Статус,b	Емкость, c	Информационный блок, r	r количество seed блоков с битами, s	Энтропия I	Количество раундов,p^a
256	128	128	2	128	12

Общий вид ГПСЧ с учетом заданных параметров представлен на рисунке 5, который состоит из этапов *параметр()*, *обновлять()* и *генерировать()*.

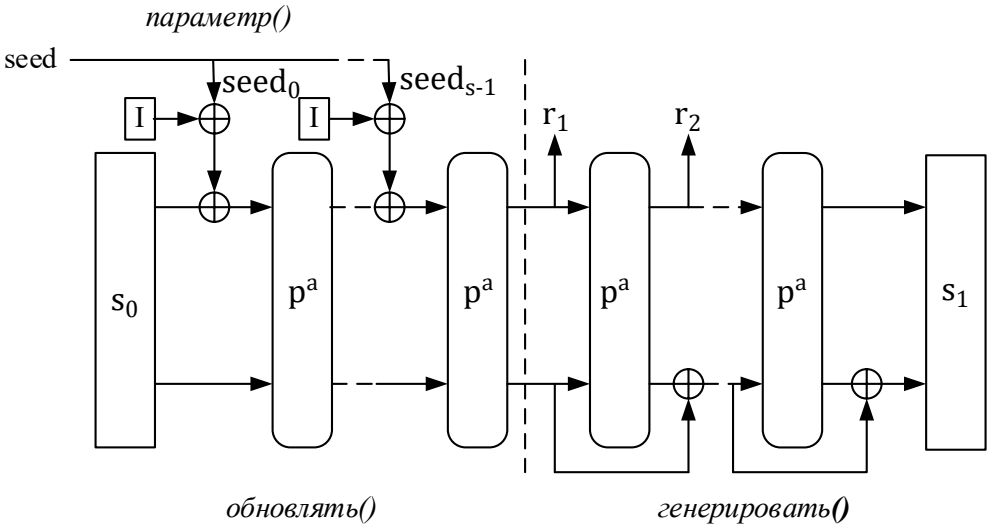


Рисунок 5. Обзор ГПСЧ на основе конструкции Sponge

Предложенный алгоритм ГПСЧ был оценен с помощью набора статистических тестов NIST в двух условиях. В первом случае набор из 100 псевдослучайных последовательностей (всего 2×10^8 бит), состоящих из 2 миллионов (2×10^6) бит, был сгенерирован с помощью разработанного программного средства с использованием различных начальных значений и значений энтропии. Во втором случае 2×10^8 бит были сгенерированы с использованием одного начального значения и энтропии и разделены на 100 частей по 2×10^6 бит. В результате анализа тесты на случайность были пройдены с результатом 96.7% в первом случае и 97.3% во втором случае.

В пятой главе диссертации, озаглавленной **«Оценка легковесных симметричных криптографических алгоритмов методами криптоанализа и результаты их реализации»**, изложены результаты оценки разработанных легковесных криптографических алгоритмов с использованием методов криптоанализа (линейного, интегрального и алгебраического), результаты их программной реализации на устройствах с различными возможностями, а также результаты внедрения разработанных программных средств на практике.

В частности, результаты линейного криптоанализа преобразования P256 показали, что все алгоритмы, основанные на нём, начиная с 3-го раунда, являются устойчивыми к линейному криптоанализу. Тот же вывод можно

сделать и для преобразований P320 и P384.

Результаты алгебраического криптоанализа показали, что из-за высокой степени уравнений по сравнению с их количеством, большого числа мономов в системе уравнений и высокой сложности её решения, 5-раундовые преобразования P256, P320 и P384 устойчивы к алгебраическому криптоанализу.

Также алгоритмы были оценены методом интегрального криптоанализа. Результаты оценки показали, что из-за невозможности выполнения обратных преобразований до входа S-таблицы на 3-м раунде после 7-го раунда, а также вследствие сложности осуществления необходимого числа выборок, 256-битный алгоритм устойчив к интегральному криптоанализу начиная с 8-го раунда, а 320-битный и 384-битный алгоритмы - начиная с 7-го раунда.

Все предложенные легковесные криптографические алгоритмы были протестированы на производительность в перечисленных ниже средах, а результаты представлены в таблице 9.

Таблица 9

Результаты программной реализации разработанных алгоритмов

Имя	Алгоритмы	Скорость шифрования/ расшифрования/хеширования/генерации, Мбайт/сек		
		Условие 1	Условие 2	Условие 3
AEAD-P320	$E, D_{128,64,12,6}$	257.149/ 246.810	41.306/ 41.322	345.620/ 340.691
AEAD-P384	$E, D_{128,128,14,8}$	212.981/ 217.124	36.367/ 36.533	336.095/ 333.150
AEAD-P384a	$E, D_{192,128,14,8}$	214.359/ 215.879	35.956/ 36.247	336.143/ 331.733
KHASH-P320	$X_{128,64,12,256}$	125.057	20.785	175.373
KHASH-P320a	$X_{192,64,12,256}$	129.995	20.788	175.283
KXOF-P320	$X_{128,64,12,0}$	132.578	20.692	176.411
KXOF-P320a	$X_{192,64,12,0}$	132.822	20.697	176.611
KHASH-P384	$X_{128,128,14,256}$	130.476	21.372	194.408
KHASH-P384a	$X_{192,128,14,256}$	129.938	21.374	193.306
KXOF-P384	$X_{128,128,14,0}$	131.730	21,373	194.414
KXOF-P384a	$X_{192,128,14,0}$	130.390	21.375	193.283
HASH-P320	$X_{0,64,12,256}$	130.305	20.787	175.390
XOF-P320	$X_{0,64,12,0}$	132.378	20.690	176.548
HASH-P384	$X_{0,128,14,256}$	131.680	21.373	194.875
XOF-P384	$X_{0,128,14,0}$	129.887	21.372	192.941
PRNG-P256	$X_{256,128,128,12}$	267.798	53.932	344.813

Условие 1: Процессор Intel(R) Core (TM) i5-10500T с тактовой частотой 2,30 ГГц, 16,0 ГБ (доступно 15,7 ГБ), 64-разрядная операционная система, процессор на базе x64, Windows 11 Pro, 24H2, mingw-gcc).

Условие 2: Raspberry Pi 4 (4 ГБ ОЗУ, 64-битный четырехъядерный процессор Cortex-A72, 2,2 ГГц, референс Raspberry Pi 2025-05-13, Debian GNU/Linux 12 (bookworm), язык программирования C, gcc 12.2.0).

Условие 3: Ubuntu 22.04.5 LTS, процессор: Intel(R) Core (TM) i5-1334U, ОЗУ: 8 ГБ, SSD 256, gcc.

Также программные средства были реализованы на 8-битном

микроконтроллере Atmega 328P (ROM: 32 Кбайт, RAM: 2 Кбайт, частота: 16 МГц, ток потребления: 9.2 мА при 5 В и 16 МГц). В таблице 10 приведены сведения об объёме памяти ROM и RAM, необходимой для реализации алгоритмов, а также данные о времени выполнения процессов и энергопотреблении для входных данных указанной длины.

Таблица 10

Результаты аппаратно-программной реализации разработанных алгоритмов

Имя	Параметры	Байт		Байт, (AD:M=(128:128)), (M=512, h=32), (L=512)	
		ПЗУ	ОЗУ	Время, мкс	Энергия, мЖ
AEAD-P320	$E, D_{128,64,12,6}$	10838	374	52329	2.407
AEAD-P384	$E, D_{128,128,14,8}$	14296	374	55965	2.427
AEAD-P384a	$E, D_{192,128,14,8}$	15344	382	56015	2.574
KHASH-P320	$X_{128,64,12,256}$	4930	308	187547	8.627
KHASH-P320a	$X_{192,64,12,256}$	4940	316	190153	8.747
KXOF-P320	$X_{128,64,12,0}$	4890	284	187547	8.627
KXOF-P320a	$X_{192,64,12,0}$	4900	292	190153	8.747
KHASH-P384	$X_{128,128,14,256}$	7038	308	171965	7.910
KHASH-P384a	$X_{192,128,14,256}$	7048	316	171965	7.910
KXOF-P384	$X_{128,128,14,0}$	6550	285	171965	7.910
KXOF-P384a	$X_{192,128,14,0}$	6560	293	171965	7.910
HASH-P320	$X_{0,64,12,256}$	4570	292	182334	8.387
XOF-P320	$X_{0,64,12,0}$	4514	268	182334	8.387
HASH-P384	$X_{0,128,14,256}$	6424	292	167316	7.697
XOF-P384	$X_{0,128,14,0}$	5906	269	167316	7.697
PRNG-P256	$X_{256,128,128,12}$	5530	284	70953	3.264

Кроме того, разработанные легковесные криптографические алгоритмы были реализованы на микроконтроллерах Arduino Mega (8-битный, Atmega-2560, ROM = 253952 байт, RAM = 8192 байт, 16 МГц, 5 В, 20,2 мА), Arduino Leonardo (8-битный, ATmega32u4, ROM = 28672 байт, RAM = 2560 байт, 16 МГц, 5 В, 12,8 мА) и Arduino DUE (32-битный, Atmel SAM3X8E ARM Cortex-M3, 84 МГц, 3,3 В, 60 мА), и были получены соответствующие результаты. Полученные данные показали, что разработанные легковесные криптографические алгоритмы могут использоваться в условиях с ограниченными ресурсами.

ЗАКЛЮЧЕНИЕ

На основе результатов исследований, проведенных в диссертационной работе по теме «Методы и алгоритмы криптографической защиты информации в системах Интернета вещей», представлены следующие выводы:

1. Нелинейные преобразования различных размеров, используемые в широко распространённых легковесных криптографических алгоритмах, были оценены на основе расширенных общих криптографических требований. Результаты оценки показали, что их показатели в части аппаратной реализации и устойчивости к атакам по побочным каналам не являются

оптимальными.

2. Метод генерации S-таблиц различных размеров на основе хаотических преобразований усовершенствован путем комбинационного использования расширенных синусных и треугольных функций. Установлено, что S-таблицы размером 4×4, 5×5, 6×6 и 8×8, полученные с помощью разработанного алгоритма на основе усовершенствованного метода, удовлетворяют высоким криптографическим требованиям.

3. На основе изучения влияния аффинного преобразования на свойства нелинейного слоя криптографического алгоритма разработан алгоритм формирования S-таблиц, устойчивых к атакам по побочным каналам и удобных для аппаратной реализации. Экспериментально показано, что S-таблицы размером 4×4, 5×5 и 6×6, созданные с помощью разработанного алгоритма формирования нелинейных преобразований, при сохранении остальных характеристик требуют меньшее количество логических элементов для аппаратной реализации по сравнению с существующими, а также обеспечивают более высокую устойчивость к атакам по побочным каналам.

4. Разработаны криптографические алгоритмы для аутентифицированного шифрования данных на основе sponge-конструкции с раундовыми преобразованиями различной длины состояния. Все разработанные алгоритмы обеспечивают 128-битную стойкость против общих атак, направленных на конструкцию, при этом алгоритм AEAD_P320 продемонстрировал наивысшую скорость среди остальных - в среднем 345.62 МБ/с.

5. Разработаны криптографические метод и алгоритмы, основанные на конструкции sponge с раундовыми преобразованиями различной длины состояний, которые генерируют хеш-значения переменной и фиксированной длины путём хеширования данных с ключом и без него. Все разработанные алгоритмы, формирующие хеш-значения фиксированной длины (256 бит), обеспечивают стойкость на уровне 128 бит, а алгоритмы, формирующие хеш-значения переменной длины (l бит), обеспечивают стойкость на уровне $min(128, l/2)$. При генерации 128-битного хеш-значения алгоритм HASH_P384 продемонстрировал наивысшую скорость - в среднем 194.875 МБ/с.

6. Разработан алгоритм генерации псевдослучайных чисел на основе sponge-конструкции, обеспечивающий высокий уровень безопасности. Результаты, полученные с использованием статистического тестового набора NIST, показали, что разработанный PTSG обеспечивает средний уровень случайности 97.3%, а скорость генерации псевдослучайных значений составляет в среднем 344.813 МБ/с.

7. Разработанные легковесные криптографические алгоритмы были оценены с использованием общих методов криптоанализа с учётом их архитектурных особенностей, а также линейного, алгебраического и интегрального криптоанализа с учётом свойств их раундовых преобразований. Результаты оценки показали, что алгоритмы обеспечивают устойчивость к линейному криптоанализу начиная с 3-го раунда, к алгебраическому

криптоанализу - начиная с 5-го раунда, и к интегральному криптоанализу - начиная с 7-го раунда.

8. Разработанные легковесные криптографические алгоритмы были протестированы на ряде 8-битных устройств Интернета вещей с ограниченными ресурсами. Результаты испытаний, проведённых на плате Arduino Mega, показали, что алгоритмы шифрования требуют до 8% памяти ROM и до 11% памяти RAM, алгоритм генерации псевдослучайных чисел - до 3% ROM и до 5% RAM, а алгоритмы хеш-функций — до 3% ROM и до 10% RAM.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

KHUDOYKULOV ZARIFJON TURAKULOVICH

METHODS AND ALGORITHMS FOR CRYPTOGRAPHIC PROTECTION OF INFORMATION IN THE INTERNET OF THINGS SYSTEM

05.01.05 – Methods and systems of information protection. Information Security

ABSTRACT OF THE DISSERTATION OF DOCTOR OF TECHNICAL SCIENCES (DSc)

Tashkent-2025

The theme of doctor of technical sciences (DSc) was registered at the Supreme attestation commission at the Ministry of higher education, science and innovation of the Republic of Uzbekistan under number B2025.3.DSc/T982.

The dissertation has been prepared at Tashkent University of Information Techologies named after Muhammad al-Khwarizmi.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of «ZiyoNet» Information and educational portal (www.ziyonet.uz).

Scientific adviser:	**Ganiyev Salim Karimovich** Doctor of technical sciences, professor
Official opponents:	**Kerimov Kamil Fikratovich** Doctor of technical sciences, professor
	Juraev Gayrat Umarovich Doctor of physical and mathematical sciences, professor
	Kuryazov Davlatyor Matyakubovich Doctor of physical and mathematical sciences
Leading organization:	**National University of Uzbekistan named after Mirzo Ulugbek**

The defense will take place on ___ _____ 20__ at ____ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.02 at Tashkent University of Information Technologies (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi (is registered under No.___). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-65-44).

Abstract of dissertation sent out on ___ _____ 20__.
(mailing report No.___ on __ _____ 20__).

B.Sh. Makhkamov
Chairman of the Scientific Council awarding scientific degrees, doctor of economic sciences, professor

M.S. Saitkamolov
Scientific secretary of Scientific Council awarding scientific degrees, doctor of economic sciences, docent

D.Ya. Irgasheva
Chairman of the Academic seminar under the Scientific Council awarding scientific degrees, doctor of technical sciences, professor

INTRODUCTION (abstract of DSc dissertation)

The purpose of the research is to improve, develop, and evaluate—using cryptanalysis methods-cryptographic methods and algorithms that ensure information security (confidentiality, integrity, and source authentication), as well as enable the generation of pseudorandom values in devices with limited capabilities.

The object of the research is the process of protecting information on resource-constrained devices.

The scientific novelty of the research is as follows:

various-sized nonlinear transformations used in existing lightweight cryptographic algorithms were evaluated based on extended general cryptographic requirements for the purpose of analyzing their security;

a method for generating S-boxes was improved through the combinational use of extended sine and tent functions in order to produce nonlinear transformations of various sizes with high security and efficient hardware implementation; moreover, an algorithm for generating S-boxes was developed by enhancing the properties of the nonlinear layer using an affine transformation;

lightweight cryptographic algorithms that ensure data confidentiality and integrity, support keys and block lengths of various sizes, and can be implemented in Internet of Things devices were developed;

lightweight cryptographic methods and algorithms that ensure data integrity and source authentication, support the generation of hash values of variable and fixed lengths, and can be implemented in Internet of Things devices were developed;

a lightweight cryptographic algorithm capable of generating sufficiently long pseudorandom sequences from a single input value, suitable for implementation in Internet of Things devices and ensuring strong security, was developed;

the developed lightweight cryptographic algorithms were evaluated using general cryptanalysis methods to determine the robustness of their structural architecture, as well as using linear, algebraic, and integral cryptanalysis methods to assess the strength of their round transformations.

Implementation of research results. Based on the scientific results obtained in the research work on the topic “Methods and algorithms for cryptographic protection of information in the Internet of Things system”:

software tools of lightweight cryptographic algorithms that include nonlinear transformations evaluated based on extended general cryptographic requirements for analyzing the security of existing lightweight cryptographic algorithms were deployed in the working environment of the southern-western branch of JSC “Uzbektelecom” for the purpose of cryptographic protection of information (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, the AEAD_P320 algorithm, which ensures data confidentiality and integrity, was found to achieve the highest speed (an average of 345.62 MB/s) compared to the others, demonstrating a speed 1.02 times higher than that of the AEAD_P384 algorithm.

software tools of lightweight cryptographic algorithms that include S-boxes

generated using an improved method based on the combinational application of extended sine and tent functions to obtain nonlinear transformations of various sizes with high security and efficient hardware implementation were deployed in the test laboratory of the State Enterprise “Cybersecurity Center” for the purpose of data protection (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, the software tool of the pseudorandom number generator was shown to enable the generation of the required pseudorandom values for cryptographic algorithms at an average speed of 53.932 MB/s.

software tools based on lightweight cryptographic algorithms that ensure data confidentiality and integrity, support keys and block lengths of various sizes, and can be implemented in Internet of Things devices were deployed in the activities of the Samarkand regional branch of the “Uzkomnazorat” Inspection for the purpose of protecting information on resource-constrained devices (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, the AEAD_P320 algorithm, which ensures data confidentiality and integrity, was shown to require on average 17.31 KB of ROM and 0.90 KB of RAM, demonstrating that it can be efficiently implemented even on 32-bit microcontrollers; moreover, all the algorithms were found to occupy no more than 3% of ROM and 2% of RAM of the microcontroller.

software tools developed on the basis of a lightweight cryptographic hash function algorithm that ensures data integrity and source authentication, and supports generating hash values of variable and fixed lengths suitable for implementation in Internet of Things devices, were deployed in the test laboratory of “UNICON.UZ – Center for Scientific, Technical, and Marketing Research” LLC on an Arduino Mega board for hashing data of various lengths (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, all algorithms were shown to require up to 3% of the microcontroller’s ROM and up to 5% of its RAM to hash 512 bytes of data, enabling the operation to be completed in 0.2 seconds with an energy consumption of 20.5 mJ.

software developed on the basis of a lightweight cryptographic algorithm capable of generating sufficiently long pseudorandom sequences from a single input value, suitable for implementation in Internet of Things devices and ensuring strong security, was deployed at “Intsoft-servis” LLC on an Arduino Leonardo board for generating pseudorandom values of various lengths (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, the pseudorandom number generation algorithm was found to occupy 34% of ROM and 21% of RAM on an 8-bit microcontroller, enabling the generation of a 256-byte value in 0.04 seconds with an energy consumption of 2.42 mJ.

software tools developed on the basis of lightweight cryptographic algorithms evaluated using general cryptanalysis methods to determine the robustness of their structural architecture, as well as linear, algebraic, and integral cryptanalysis methods to assess the strength of their round transformations, were deployed in the

test laboratory of “UNICON.UZ – Center for Scientific, Technical, and Marketing Research” LLC (the reference of the Ministry of Digital Technologies No.33-8/6636, September 17, 2025). As a result of the scientific study, the proposed algorithms were shown to provide resistance to linear, algebraic, and integral cryptanalysis methods, while also allowing implementation on 8-bit microcontrollers with minimal memory requirements.

Structure and volume of the dissertation. The composition of the dissertation consists of an introduction, five chapters, a conclusion, a list of used literature and appendices. The length of the dissertation is 174 pages.

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

I bo‘lim (I часть; I part)

1. Khudoykulov Z. A Comparison of Lightweight Cryptographic Algorithms // Lecture Notes in Networks and Systems, Vol 912, Springer, https://doi.org/10.1007/978-3-031-53488-1_36, –P. 295-304. (11, Springer).
2. Safoev N., Khan A., Khudoykulov Z., Arya R. Energy-Efficient Implementation of BCD to Excess-3 Code Converter for Nano-Communication Using QCA Technology // China Communications. Volume 21, Number 6, 2024. -P. 103-111. (3, Scopus).
3. Das R., Khan A., Arya R., Boykuziev I., Abdurakhimov B., Safoyev N., Khudoykulov Z. SSKA: secure symmetric encryption exploiting Kuznyechik algorithm for trustworthy communication // International Journal of “System Assurance Engineering and Management”. Volume 15, 2024. -P. 2391-2400. (3, Scopus).
4. Khudoykulov Z., Shirinov L. Analysis of Security Protocols in Wireless Sensor Networks // International Conference on “Information Science and Communications Technologies (ICISCT)”. Tashkent, Uzbekistan-2019. -4p. (OAK Rayosatining 30.09.2019-yildagi 269/8-qarori dissertatsiyalar asosiy ilmiy natijalarini e’lon qilishga tavsiya etilgan xorijiy ilmiy nashrlarda chop etilgan ilmiy maqolalarga tenglashtirilgan, (3) Scopus).
5. Ganiev S., Khudoykulov Z. Lightweight Cryptography Algorithms for IoT Devices: Open issues and challenges // International Conference on “Information Science and Communications Technologies (ICISCT)”, Tashkent, Uzbekistan-2021. -4p. (OAK Rayosatining 30.10.2021-yildagi 525-qarori dissertatsiyalar asosiy ilmiy natijalarini e’lon qilishga tavsiya etilgan xorijiy ilmiy nashrlarda chop etilgan ilmiy maqolalarga tenglashtirilgan, (3) Scopus).
6. Abdurakhimov B., Allanov O., Boykuziev I., Khudoykulov Z. Differential Collisions in SHA-1 // International Conference on “Information Science and Communications Technologies (ICISCT)”, Tashkent, Uzbekistan-2020. -5p. (OAK Rayosatining 30.10.2020-yildagi 368-qarori dissertatsiyalar asosiy ilmiy natijalarini e’lon qilishga tavsiya etilgan xorijiy ilmiy nashrlarda chop etilgan ilmiy maqolalarga tenglashtirilgan, (3) Scopus).
7. Худойкулов З.Т., Тожиакбарова У.У., Болтаев Ф.Ҳ. Дастурий кўринишда амалга оширишга қулай оқимли шифрлаш алгоритми // “Ахбороткоммуникациялар: Тармоқлар, Технологиялар, Ечимлар” ҳар чораклик илмий-техник журнал. № 1(57), 2021. –Б. 35-43. (05.00.00; №2).
8. Худойкулов З.Т., Ортиқбоев А.М., Турсунов О.О., Файзирахмонов Б.Б. Буюмлар интернети тизимларида хавфсизлик муаммолари // “Ахбороткоммуникациялар: Тармоқлар, Технологиялар, Ечимлар” ҳар чораклик илмий-техник журнал. № 4(60), 2021. –Б. 27-34. (05.00.00; №2).

9. Худойкулов З.Т., Ортиқбоев А.М. Енгил блокли симметрик шифрлаш алгоритмларини лойиҳалаш усулларининг таҳлили // “Ахбороткоммуникациялар: Тармоқлар, Технологиялар, Ечимлар” ҳар чораклик илмий-техник журнал. № 1(65), 2023. –Б. 26-31. (05.00.00; №2).

10. Xudoykulov Z.T., Rahmatullayev I.R. Yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlar tahlili // “Raqamli texnologiyalarning nazariy va amaliy masalalari” xalqaro jurnali. №7(2), 2024. -B. 51–58. (05.00.00; OAK Rayosatining 2023-yil 29-avgustdagi 342/5-son qarori).

11. Xudoykulov Z.T. Xaotik akslantirishga asoslangan s jadvallarni hosil qilish algoritmi // “Raqamli Transformatsiya va Sun’iy Intellekt” ilmiy jurnali. VOLUME 2, ISSUE 3, 2024. -B. 51-63. (05.00.00; OAK Rayosatining 2023-yil 4-iyuldagi 340/5-son qarori).

12. Ganiyev S.K., Xudoykulov Z.T. Faktorlash asosida S jadvallarni apparat amalga oshirilishni takomillashtirish // “Raqamli texnologiyalarning nazariy va amaliy masalalari” xalqaro jurnali. №7(3), 2024. -B. 93–99. (05.00.00; OAK Rayosatining 2023-yil 29-avgustdagi 342/5-son qarori).

13. Xudoykulov Z.T., Qozoqova T.Q. Present yengil vaznli kriptografik algoritmining tahlili // “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali. Tom 1, Son 4, 2024. -B. 152-157. (05.00.00; OAK Rayosatining 2023-yil 30-sentyabrdagi 343-son qarori).

14. Xudoykulov Z.T. Affin akslantirishining S-jadval xususiyatlariga ta’siri // “Axborot xavfsizligi muammolari” ilmiy jurnali. № 1(2), 2025. -B. 5-15. (05.00.00; OAK Rayosatining 2024-yil 30-noyabrdagi 1099-son qarori).

15. Xudoykulov Z.T. Sponge konstruksiyasi uchun bardoshli akslantirishlar // “Axborot xavfsizligi muammolari” ilmiy jurnali. № 2(3), 2025. -B. 38-49. (05.00.00; OAK Rayosatining 2024-yil 30-noyabrdagi 1099-son qarori).

II bo‘lim (II часть; II part)

16. Khudoykulov Z. Hardware and software implementation of lightweight cryptography algorithms // International Conference on “Advance Research in Humanities, Applied Sciences and Education”. Germany-2025. –P. 37-43.

17. Khudoykulov Z. Security analysis of sponge constructions // International Conference on “Advance Research in Humanities, Applied Sciences and Education”. Spain-2025. –P. 30-36.

18. Khudoykulov Z. Opportunities of sponge construction in cryptographic systems: design settings and security considerations // Next Scientists Conferences “The future of work: social science insights on labor and employment trends”. USA-2025. -P. 190-194.

19. Худойқулов З.Т. Қуролли кучлар тизимида IoT технологиясидан фойдаланиш // “Qurolli kuchlar tuzilmalarini innovatsion rivojlantirishda axborot-kommunikatsiya texnologiyalarining o‘rni” mavzusidagi respublika ilmiy-uslubiy onlayn konferensiyasi maqolalar to‘lami. 1-qism. Toshkent-2021. -Б. 67-70.

20. Xudoyqulov Z.T., Fayziraxmonov B.B. IoT tizimlarida mavjud xavfsizlik muammolari // “Hududlarda raqamli iqtisodiyotni rivojlantirish istiqbollari:

muammolar va yechimlar”respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami. Qarshi-2021. -B. 294-296.

21. Худойкулов З., Файзирахмонов Б. IoT хавфсизлигини таъминлашда криптографиянинг ўрни // “Zamonaviy axborot, kommunikatsiya texnologiyalari va at-ta’lim tatbiqi muammolari” mavzusidagi respublika ilmiy-amaliy anjumani ma’ruzalar to‘plami, 1-tom. Samarqand-2021. -Б. 202-204.

22. Худойкулов З. IoT қурилмалари таснифи // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumani ma’ruzalar to‘plami. 1-qism. Toshkent-2022. –Б. 340-342.

23. Xudoykulov Z.T. Yengil vaznli kriptografik algoritmlarni standartlashtirish holati // “Yangi O‘zbekistonda axborotlashgan jamiyatni rivojlantirish istiqbollari: muammolar va imkoniyatlar” ilmiy-nazariy anjuman materiallari to‘plami. Toshkent-2024. -B. 609-613.

24. Xudoykulov Z.T. Buyumlar interneti xavfsizligi sohasida dolzarb tadqiqot mavzulari // “Kompyuter ilmlari va muhandislik texnologiyalari” xalqaro ilmiy-texnik konferensiya materiallari to‘plami. 2-qism. Jizzax-2022. –B. 7-9.

25. Xudoykulov Z.T. Buyumlar internetining zamonaviy foydalanish sohalari // «Professional armiya boshqaruvini rivojlanishida innovatsiyalar va raqamlashtirishning o‘rni» VII xalqaro ilmiy-amaliy konferensiya maqolalar to‘plami. 1-qism. Toshkent-2025. -B. 279-285.

26. Худойкулов З. Симметрик блокли “енгил” шифрлаш алгоритмлари // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati” Respublika ilmiy-texnik anjumani ma’ruzalar to‘plami, 1-qism. Toshkent-2022. –Б. 342-343.

27. Ganiyev S.K., Xudoykulov Z.T. SBH xeshlash algoritmlari oilasi // O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 54323. Toshkent, 26.08.2025.

28. Ganiyev S.K., Xudoykulov Z.T., Rahmatullayev I.R. SboxGates: S jadvallarni amalga oshirishdagi mantiqiy elementlar sonini aniqlash dasturi // O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 41977. Toshkent, 20.08.2024.

29. Ganiyev S.K., Xudoykulov Z.T. SBPrng algoritmi // O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 54322. Toshkent, 26.08.2025.

30. Ganiyev S.K., Xudoykulov Z.T. SBA shifrlash algoritmlari oilasi // O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 54324. Toshkent, 26.08.2025.

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

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 4,25. Adadi 100 dona. Buyurtma № 29/24.

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