OQIMLI SHIFRLASH ALGORITMLARINING TAHLILI

Qozoqova To‘xtajon Qaxramon qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, “Kriptologiya” kafedrasi assistenti, Toshkent, O‘zbekiston
E-mail: qozoqovat1516@gmail.com
https://orcid.org/0009-0000-3938-3879

Annotatsiya: Ushbu maqolada IoT qurilmalarida oqimli shifrlash algoritmlarining o‘rni va ularning matematik asoslari tahlil qilingan. Tadqiqotda sinxron va o‘z-o‘zidan sinxronlanuvchi oqimli shifrlarning ishlash mexanizmlari, ularning afzalliklari hamda xavfsizlik jihatlari yoritilgan. Asosiy e’tibor LFSR, Galua maydonlari, va ARX operatsiyalariga asoslangan oqimli shifrlash modellariga qaratilgan. Shuningdek, eSTREAM tanlovida tavsiya etilgan yengil oqimli shifrlar (Trivium, Grain, ChaCha20) IoT muhitida samarali yechim sifatida baholangan. Natijalar IoT tizimlari uchun yengil, xavfsiz va samarali oqimli shifrlarni ishlab chiqish zarurligini ko‘rsatadi.

Kalit so‘zlar: IoT, oqimli shifrlash, sinxron shifr, LFSR, Galua maydoni, Trivium, Grain, ChaCha20, yengil kriptografiya, psevdo-tasodifiy generator.

Аннотация. В данной статье проанализирована роль потоковых шифров в устройствах Интернета вещей (IoT) и их математические основы. В исследовании рассмотрены механизмы работы синхронных и самосинхронизирующихся потоковых шифров, их преимущества и аспекты безопасности. Основное внимание уделено моделям потокового шифрования, основанным на LFSR, полях Галуа и ARX-операциях. Также оценены лёгкие потоковые шифры (Trivium, Grain, ChaCha20), рекомендованные в рамках проекта eSTREAM, как эффективные решения для IoT-среды. Результаты показывают необходимость разработки лёгких, безопасных и эффективных потоковых шифров для IoT-систем.

Ключевые слова: IoT, потоковое шифрование, синхронный шифр, LFSR, поле Галуа, Trivium, Grain, ChaCha20, лёгкая криптография, псевдослучайный генератор.

Abstarct. This article analyzes the role of stream ciphers in Internet of Things (IoT) devices and their mathematical foundations. The study examines the operating mechanisms of synchronous and self-synchronizing stream ciphers, their advantages, and security aspects. The main focus is on stream cipher models based on LFSR, Galois fields, and ARX operations. Lightweight stream ciphers (Trivium, Grain, ChaCha20) recommended by the eSTREAM project are also evaluated as effective solutions for the IoT environment. The results demonstrate the need to develop lightweight, secure, and efficient stream ciphers for IoT systems.

ISSN 3030-3907

Key words: IoT, stream cipher, synchronous cipher, LFSR, Galois field, Trivium, Grain, ChaCha20, lightweight cryptography, pseudorandom generator.

Kirish

So‘nggi yillarda Buyumlar interneti (IoT) texnologiyasi jadal rivojlanib, dunyo bo‘yicha milliardlab qurilmalarni yagona tarmoqqa ulanmoqda. Ushbu qurilmalar turli sohalarda sog‘liqni saqlash, transport, sanoat, aqlli uylar va xavfsizlik tizimlarida real vaqt rejimida ma’lumot almashadi. Biroq, bu jarayon bilan birga axborot xavfsizligi, maxfiylik, va ma’lumot yaxlitligini ta’minlash dolzarb muammolardan biri bo‘lib qolmoqda. IoT qurilmalarining asosiy cheklovi ya’ni ularning resurslari xotira, energiya, protsessor tezligi juda pastligidadir. Shu sababli, murakkab kriptografik algoritmlar, masalan, AES, RSA yoki ECC, ko‘p hollarda samarali ishlamaydi. Shu nuqtai nazardan, oqimli shifrlash algoritmlari yengil va tezkor ishlash xususiyati bilan ajralib turadi hamda IoT tizimlarida samarali yechim sifatida qaraladi.

IoT tizimlarida oqimli shifrlash algoritmlarining o‘rni. Oqimli shifrlash algoritmlari bu bitma-bit yoki baytma-bayt shifrlashni amalga oshiruvchi yengil kriptografik tizimlardir. Ular kalit oqimini hosil qilib, ochiq matn bilan XOR amali orqali shifrlangan ma’lumotni yaratadi. Shu sababli, bu turdagi shifrlashlar kam resursli IoT qurilmalar uchun juda qulaydir. IoT muhitida keng qo‘llanilayotgan oqimli shifrlash algoritmlariga quyidagilar kiradi. Trivium, Grain, MICKEY, Ascon, TinyJAMBU. Ular NIST Lightweight Cryptography Competition tanlovida yengil kriptografiya uchun tavsiya etilgan algoritmlar sirasiga kiradi. Bugungi kunda IoT tarmoqlarida milliardlab qurilmalar bir vaqtda ishlayotgani sababli, ularning har biri ishonchli shifrlash mexanizmlariga ega bo‘lishi zarur. Oqimli shifrlash algoritmlari IoT muhitida xavfsizlikni ta’minlash bilan birga, energiyani tejaydi, real vaqtli uzatishni qo‘llab-quvvatlaydi va kichik apparat arxitekturalarida ishlay oladi. Shu sababli, ularning matematik asoslarini takomillashtirish va kriptoanalizga chidamli modellar ishlab chiqish bugungi kunda ilmiy jihatdan eng dolzarb yo‘nalishlardan biri hisoblanadi.

ADABIYOTLAR TAHLILI

Oqimli shifrlash algoritmlarining muammolar va kamchiliklarini bilish va tahlil qilish uchun shu borada yopzilgan bir necha maqolalar tahlil qilindi jumladan bu borada ish olib borgan chet el olimlari o‘rganib chiqildi. Frederik Armknecht, Matthias Krause [1] tomonidan yozilgan maqolada oqimli shifrlar turlari, ularning zaifliklari jumladan chiziqlilik, korrelyatsiya hujumlari va zamonaviy kriptotahlil usullari algebraik hamda statistik kriptotahlil to‘g'risida keng yoritilgan. Mazkur muammolarni chuqur tahlil qiluvchi asosiy ilmiy manbalardan biri Douglas R. Stinsonning Cryptography: Theory and Practice asaridir [2]. Ushbu kitobda muallif oqimli shifrlar asosini tashkil qiluvchi Vernam shifri haqida batafsil to‘xtalib,

ISSN 3030-3907

uning ideal xavfsizligi faqat kalit hech qachon qayta ishlatilmasa va haqiqiy tasodifiy bo‘lsa ta'minlanishini ta'kidlamoqda. Shu bilan birga, amaliyotda haqiqiy tasodifiy kalitlarni uzun muddat saqlash va taqsimlash qiyin bo‘lgani uchun ko‘pincha pseudo-tasodifiy generatorlar (PRG) qo‘llaniladi. Stinson shu PRG larning matematik jihatdan zaif bo‘lishi masalan, chiziqli qaytaruvchan registr (LFSR) asosidagi generatorlarning Berlekamp Massey algoritmi yordamida qisqa chiqish ketma-ketligidan butun tuzilma qayta tiklanishi mumkinligini ko‘rsatadi.

Yana bir muhim manba Jonathan Katz va Yehuda Lindellning [3] asaridir. Ular oqimli shifrlarning xavfsizligini kriptografik PRG tushunchasi orqali formalizatsiya qiladi. Mualliflar kalitning qayta ishlatilishi natijasida shifrlangan ikkita xabar XOR qilinsa, dushman ularning mazmunini qisman yoki to‘liq aniqlashi mumkinligini misollar orqali tushuntiradi. Bu muammoni hal qilish uchun har bir sessiya uchun nonce yoki IV (initialization vector) ishlatish tavsiya etiladi.

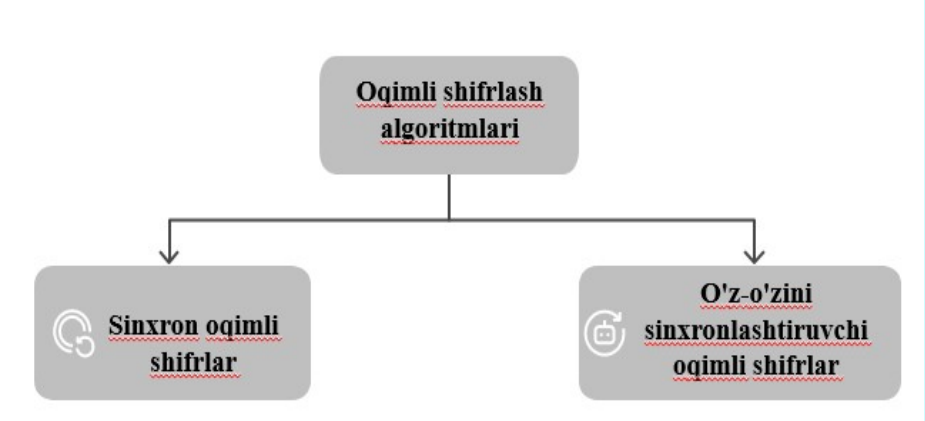
Bart Preneelning [4] nomli ishida esa zamonaviy oqimli shifrlar (RC4, Salsa20, ChaCha20) tahlil qilinadi. RC4 algoritmi keng qo‘llanilgan bo‘lsada, uning statistik zaifliklari (masalan, ba'zi baytlarning ehtimoliy taqsimoti tekis emasligi) tufayli ko‘plab xavfsizlik buzilishlariga sabab bo‘lgan. Buni hal qilish maqsadida Salsa20 va ChaCha20 kabi yangi avlod oqimli shifrlar ishlab chiqilgan bo‘lib, ular yuqori tezlik, sodda tuzilma hamda kuchli kriptografik xavfsizlikka ega. ChaCha20, ayniqsa, Google tomonidan TLS protokollarida qo‘llanilish uchun tavsiya etilgan va IETF standarti (RFC 8439) sifatida qabul qilingan. ECRYPT II (European Network of Excellence in Cryptology) tomonidan nashr etilgan [5] "The eSTREAM Portfolio" ham oqimli shifrlar sohasidagi muhim ilmiy loyiha hisoblanadi. Ushbu loyiha doirasida dunyoning yetakchi kriptograflari tomonidan taklif etilgan 34 ta oqimli shifrdan 8 tasi (Grain-128a, Trivium, HC-128) xavfsizlik, samaradorlik va amalga oshirish qobiliyati jihatidan eng yaxshi sifatida tanlangan. Bu tanlov jarayonida kalit qayta ishlatish, nonce qayta ishlatish, hamda ichki holatga hujum qilish kabi muammolar tizimli ravishda baholangan.

TADQIQOT METODOLOGIYASI

Oqimli shifrlash algoritmlari – bu ma'lumotlarni bitma-bit yoki baytma-bayt shifrlaydigan simmetrik shifrlash usullari. Ular ochiq matnni (plaintext) psevdo-tasodifiy kalit oqimi (keystream) bilan XOR operatsiyasi orqali shifrlaydi. Bu usul katta hajmdagi ma'lumotlarni tez shifrlash uchun samarali. Bu algoritmlar Vernam shifrining psevdo-tasodifiy versiyasiga asoslanadi, Shannonning mukammal maxfiylik nazariyasiga muvofiq, kalit oqimi to‘liq tasodifiy bo‘lsa, shifr buzilmaydi. Ammo amalda psevdo-tasodifiy generatorlar ishlatiladi, bu esa xavfsizlikni generatorning sifatiga bog'laydi.

ISSN 3030-3907

Oqimli shifrlarni quyidagi turlarga bo‘lish mumkin, har biri ma’lumotlar oqimi va kalit generatsiyasiga bog'liq bo‘lib aynan shu nuqtai nazardan ularni 1-rasmda keltirilgan kabi turlari mavjud buni.



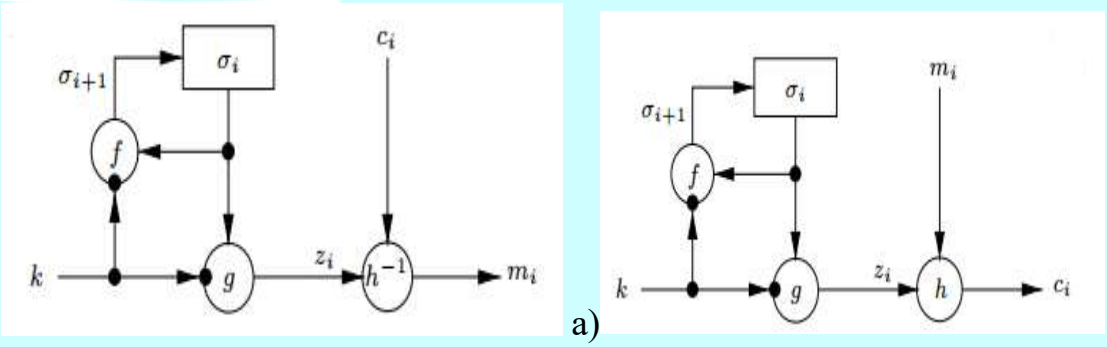
1-rasm. Oqimli shifrlash algoritmlari turlari

Sinxron oqim shifri bu kalit oqimi (keystream) matn va shifrlangan matndan mustaqil ravishda hosil qilinadigan shifrdir.

Sinxron oqim shifrining shifrlash jarayoni quyidagi tenglamalar orqali ifodalanadi:

$$\sigma_{i+1} = f(\sigma_i, k)$$
$$z_i = g(\sigma_i, k)$$
$$c_i = h(z_i, m_i)$$

Bu yerda σ_0 dastlabki holat bo‘lib, u kalit k orqali aniqlanadigan, f keyingi holat funksiyasi, g kalit oqimi z_i ni hosil qiluvchi funksiya, h esa kalit oqimi va ochiq matn m_i ni birlashtirib, shifrlangan matn c_i ni hosil qiluvchi chiqish funksiyasidir. 2-rasmda sinxron oqimli shifrlash algoritmini a) deshifrlash b) rasm esa shifrlash modelidir.



a) b)

2-rasm. Sinxron oqimli shifrning umumiy modeli a) deshifrlash, b) shifrlash

Sinxron oqimli shifrlarning xususiyatlari

(i) Sinxronizatsiya talablari. Sinxron oqimli shifrlarda yuboruvchi va qabul qiluvchi bir xil kalitdan foydalanishi va shu kalitdagi bir xil holatda ishlashi kerak, shunda to‘g‘ri deshifrlash amalga oshadi. Agar uzatish vaqtida shifrlangan belgilar kiritilsa yoki o‘chirib tashlansa, sinxronizatsiya buziladi va deshifrlash muvaffaqiyatsiz bo‘ladi. Uni tiklash uchun qo‘shimcha sinxronizatsiya texnikalari qo‘llaniladi. Bunga qayta ishga tushirish shifrlangan matnda ma’lum oraliqlarda

ISSN 3030-3907

maxsus belgilarni joylashtirish yoki agar ochiq matnda yetarlicha takroriylik bo‘lsa, barcha mumkin bo‘lgan kalit oqimi siljishlarini sinab ko‘rish kiradi.

(ii) Xatoliklarning tarqamasligi. Uzatish jarayonida o‘zgartirilgan (lekin o‘chirib tashlanmagan) shifrlangan belgining xatosi boshqa belgilarni deshifrlash jarayoniga ta’sir qilmaydi.

(iii) Faol hujumlar. (i)-xususiyat natijasida faol hujumchi tomonidan shifrlangan belgilarni qo‘shish, o‘chirish yoki qayta yuborish sinxronizatsiyaning darhol yo‘qolishiga olib keladi, bu esa deshifrlovchi tomonidan aniqlanishi mumkin. (ii)-xususiyat natijasida faol hujumchi ayrim shifrlangan belgilarni o‘zgartirib, bu o‘zgarishlarning ochiq matnga qanday ta’sir qilishini aniq bilishi mumkin. Bu holat ma’lumotning manbaini autentifikatsiya qilish va yaxlitligini kafolatlash uchun qo‘shimcha mexanizmlar kerakligini ko‘rsatadi.

O‘z-o‘zidan sinxronlanuvchi oqimli shifrlar

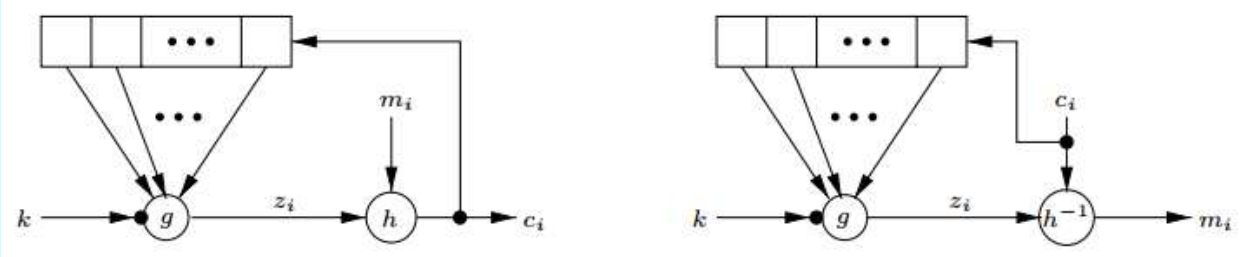
O‘z-o‘zidan sinxronlanuvchi yoki asinxron oqimli shifr bu shunday shifrki, unda kalit oqimi kalit va oldingi shifrlangan belgilar soni bilan cheklangan miqdordagi qiymatlar asosida hosil qilinadi.

Bunday shifrning shifrlash funksiyasi quyidagi tenglamalar bilan ifodalanadi:

$$\sigma_i = (c_{i-t}, c_{i-t+1}, \dots \dots, c_{i-1})$$
$$z_i = g(\sigma_i, k)$$
$$c_i = h(z_i, m_i)$$

Bu yerda $\sigma_i = (c_{i-t}, c_{i-t+1}, \dots \dots, c_{i-1})$ maxfiy bo‘lmagan dastlabki holat, kalit k, g kalit oqimi z_i ni hosil qiluvchi funksiya, h esa kalit oqimi va ochiq matn m_i ni birlashtirib, shifrlangan matn c_i ni hosil qiluvchi chiqish funksiyasidir.

Shifrlash va deshifrlash jarayonlari 3-rasmda keltirilgan.Hozirda eng ko‘p qo‘llaniladigan o‘z-o‘zidan sinxronlanuvchi oqimli shifrlar blokli shifrlashning 1-bitli teskari aloqa rejimi (cipher feedback mode) asosida qurilgan.



a) **b)**

3-rasm. O‘z-o‘zidan sinxronlanuvchi oqimli shifrlarning a)shifrlash b)deshifrlash modeli

O‘z-o‘zidan sinxronlanuvchi oqimli shifrlarning xususiyatlari.

(i) O‘z-o‘zidan sinxronlanish. Agar shifrlangan belgilar uzatish jarayonida o‘chirib tashlansa yoki kiritilsa ham, o‘z-o‘zidan sinxronlanuvchi shifrlar to‘g‘ri deshifrlashni avtomatik tarzda tiklay oladi, chunki deshifrlash jarayoni faqat oldingi belgilar soni bilan chegaralangan shifrlangan belgilar to‘plamiga bog‘liq

ISSN 3030-3907

bo‘ladi. Sinxronizatsiya yo‘qolgandan keyin ma’lum miqdordagi ochiq matn belgilarini tiklab bo‘lmaydi, lekin undan keyin tizim o‘zini tiklaydi.

(ii) Xatoliklarning cheklangan tarqalishi. Agar o‘z-o‘zidan sinxronlanuvchi oqimli shifr holati t ta oldingi shifrlangan belgiga bog‘liq bo‘lsa, uzatish jarayonida bitta shifrlangan belgi o‘zgartirilsa (yoki o‘chirib tashlansa, kiritilsa), u holda navbatdagi t ta shifrlangan belgining deshifrlanishi noto‘g‘ri bo‘ladi. Shundan so‘ng to‘g‘ri deshifrlash qayta tiklanadi.

(iii) Faol hujumlar (ii)-xususiyatga ko‘ra, faol hujumchi tomonidan shifrlangan belgilarni o‘zgartirish bir nechta belgilarni noto‘g‘ri deshifrlanishiga olib keladi, bu esa sinxron oqimli shifrlarga nisbatan hujumni aniqlash ehtimolini oshiradi. Ammo (i)-xususiyat tufayli, faol hujumchi tomonidan belgilarni kiritish, o‘chirish yoki qayta yuborishni aniqlash sinxron shifrlarga qaraganda qiyinroq bo‘ladi. Bu holat ma’lumotning manbasini tasdiqlash va yaxlitligini ta’minlash uchun qo‘shimcha mexanizmlar zarurligini ko‘rsatadi.

(iv) Ochiq matn statistikasi tarqalishi. Har bir ochiq matn belgisi keyingi barcha shifrlangan belgilarni ta’sir qiladi, shuning uchun ochiq matnning statistik xususiyatlari shifrlangan matn bo‘ylab tarqaladi. Natijada, o‘z-o‘zidan sinxronlanuvchi oqimli shifrlar ochiq matnning takrorlanishiga asoslangan hujumlarga nisbatan sinxron oqimli shifrlarga qaraganda bardoshlirroq bo‘lishi mumkin.

Sinxron oqimli shifrlash algoritmlarini LFSR asosidagi qurilishi

Ko‘p sinxron oqimli shifrlar chiziqli qayta bog‘lanishli siljitish registrlari (LFSR -Linear Feedback Shift Registers) ga asoslanadi [6][7]. LFSR bu ketma-ket bitlar generatori bo‘lib, u chiziqli algebra va Galua maydonlari (Finite Fields) nazariyasiga tayanadi [6].

LFSR ning matematik modeli:

$$s_{i+t} = c_1 s_{i+t-1} \oplus c_2 s_{i+t-2} \oplus \dots \dots \oplus c_1 s_i$$

Bu yerda s_i registrdagi bitlar holati, $c_i\{0,1\}$ koeffitsientlar, amallar GF(2) (ya’ni mod 2) maydonda bajariladi [6]. Galua maydoni (GF(2)) bu ikkilik arifmetika sohasi bo‘lib, barcha amallar mod 2 da bajariladi [6]:

$$1 + 1 = 0$$
$$1 \times 1 = 1$$
$$1 + 0 = 1$$

Shuning uchun LFSR chiziqli algebra asosida ketma-ket bitlar hosil qiladi [2]. Sinxron oqimli shifrlarning nazariy poydevori quyidagi fanlarga tayanadi:

1. Chiziqli algebra LFSR strukturasini tashkil etuvchi tenglamalar chiziqli rekurrent sistemalardir [6].
2. Galua maydonlari (Finite Fields) barcha amallar GF(2^n) maydonida bajariladi, bu esa deterministik va periodik xususiyat beradi [6].

ISSN 3030-3907

3. Diskret matematika va avtomatlar nazariyasi oqim ketma-ketligi deterministik avtomat sifatida modellashtiriladi [7].

1-jadval.

Sinxron oqimli shifrlash algoritmlariga misollar

Algoritm	Yil	Xususiyat	Qo‘llanilishi
RC4	1987	Dastlabki mashhur oqimli shifr	TLS, WEP
Trivium	2005	Yengil apparat shifr	IoT
Grain v1	2006	Yengil sinxron oqimli shifr	Sensor tarmoqlar
Salsa20/ChaCha20	2005	Tez va xavfsiz shifr	TLS 1.3, VPN

TAHLIL VA NATIJALAR

Qanday matematik muammolarga asoslangan? Ushbu savolga javob topish oldimizga qo‘yilgan asosiy maqsad bo‘lib belgilandi. Oqimli shifrlarning xavfsizligi quyidagi matematik muammolarga asoslanadi, ular psevdo-tasodifiy generatorlarning bashorat qilib bo‘lmasligini ta'minlaydi:

- Psevdo-tasodifiy sonlar generatsiyasi (PRNG): Kalit oqimi tasodifiy ko‘rinishi kerak, bu esa tasodifiylik testlariga (masalan, NIST SP 800-22) asoslanadi. Muammo: Generatorning davrini va chiziqliligini bashorat qilish qiyinligi.

- Chiziqli teskari aloqa registrlari (LFSR): Ko‘p oqimli shifrlar LFSR ga asoslanadi, ular polinomlar va Galua maydonlari (GF(2)) ustidagi chiziqli algebra muammolariga tayanadi. Muammo: Berlekamp-Massey algoritmi orqali LFSR ni qayta tiklashning murakkabligi (NP-hard yaqin).

- Bir tomonlama funktsiyalar (One-way functions): Ba'zi zamonaviy shifrlar (masalan, ChaCha20) hash funktsiyalarga asoslanadi, ularning teskari hisoblash qiyinligi (preimage resistance) P vs NP muammosiga bog'liq.

- Diskret logarifm muammosi: Ba'zi shifrlar (masalan, Blum-Blum-Shub) bu muammoga asoslanadi, lekin oqimli shifrlarda kamroq ishlatiladi. Ilmiy asos: Bu muammolar kriptografiyaning asosiy postulatlaridir, Rivest va boshqalar tomonidan ishlab chiqilgan. Oldingi maqolalarda eSTREAM tanlovida golib bo‘lgan algoritmlar tahlil qilingan va ulardan bir nechtasi tanlab olindi va tahlil qilish uchun 1-jadvalda keltirildi.

ISSN 3030-3907

1-jadval.

Oqimli shifrlash algoritmlar tahlili

Algoritm nomi	Tur	Matematik asos	Ilmiy tavsif
RC4	Sinxron	LFSR va permutatsiyalar	Ron Rivest tomonidan ishlab chiqilgan, 256 baytlik S-box ga asoslanadi. Xavfsizligi psevdo-tasodifiy permutatsiyalarning bashorat qilish qiyinligiga bog'liq.
A5/1	Sinxron	Bir nechta LFSR registrlari	GSM telefonlarida ishlatiladi, 3 ta LFSR (19, 22, 23 bit) dan iborat. Matematik asos: Chiziqli algebra va Berlekamp-Massey algoritmi.
Salsa20	Sinxron	ARX operatsiyalari (Add-Rotate-XOR)	Daniel Bernstein tomonidan ishlab chiqilgan, 32-bit so‘zlar ustidagi arifmetik operatsiyalarga asoslanadi.
ChaCha20	Sinxron	ARX va kvartet operatsiyalari	Salsa20 ning takomillashtirilgan versiyasi, Bernstein tomonidan. Matematik asos: Katta sonlar ustidagi modul arifmetikasi va psevdo-tasodifiylik.
Grain	Sinxron	LFSR va NLR (Non-Linear Feedback	eSTREAM loyihasida tanlangan, 80-bit kalit. Asos: Chiziqli va chiziqsiz filtrlar, Berlekamp-Massey ga qarshilik

ISSN 3030-3907

XULOSA

IoT texnologiyalarining keng qo‘llanilishi bilan birga, yengil, xavfsiz va samarali shifrlash algoritmlariga ehtiyoj keskin ortmoqda. Oqimli shifrlash algoritmlari ushbu talabni qondiruvchi eng maqbul yechimlardan biri bo‘lib, ularning asosiy ustunligi yuqori tezlik, kam resurs sarfi va real vaqtli ishlash imkoniyatidir. Tahlillar shuni ko‘rsatadiki:

- Sinxron oqimli shifrlar (Trivium, Grain, ChaCha20) IoT qurilmalarida samarali ishlaydi, biroq sinxronizatsiya buzilishi xavfi mavjud.
- O‘z-o‘zidan sinxronlanuvchi shifrlar (masalan, CFB rejimidagi modellarga asoslanganlar) xatoliklarni cheklangan tarzda tarqatadi va uzatishdagi uzilishlardan tez tiklanadi.
- LFSR va Galua maydoni nazariyasiga asoslangan shifrlar (Grain, A5/1) oddiy apparat strukturasiga ega, ammo chiziqli kriptoanalizga nisbatan zaifliklar mavjud.
- ARX operatsiyalariga asoslangan algoritmlar (Salsa20, ChaCha20) kuchli tasodifiylik va yuqori xavfsizlikni ta’minlaydi, shuning uchun ular zamonaviy internet protokollarida keng qo‘llanmoqda. Shu asosda, IoT tizimlari uchun oqimli shifrlash algoritmlarini tanlashda quyidagi mezonlar muhim:

- energiya samaradorligi,
- apparat soddaligi,
- kriptotahlilga bardoshlilik,
- kalit va IV boshqaruvi.

Kelgusi tadqiqod ishlarimda oqimli shifrlarni matematik asoslarini (PRNG, LFSR, ARX) yanada optimallashtirish, ularni gibrid autentifikatsiya mexanizmlari bilan integratsiya qilish IoT xavfsizligini oshirishda muhim ilmiy yo‘nalish bo‘lib qoladi.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI

1. Armknecht, F., & Krause, M. (2003). Algebraic attacks on combiners with memory. *In D. Boneh (Ed.), Advances in Cryptology – CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 2003. Proceedings* (pp. 162–176). Springer. https://doi.org/10.1007/978-3-540-45146-4_10

2. Katz, J., & Lindell, Y. (2020). Introduction to modern cryptography (3rd ed.). CRC Press. Preneel, B. (2013). Stream ciphers and their applications. Springer. Stinson, D. R. (2018). Cryptography: Theory and practice (4th ed.). CRC Press. The eSTREAM Project. (2011). The eSTREAM portfolio. European Network of Excellence in Cryptology II (ECRYPT II). https://www.ecrypt.eu.org/stream/

3. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. *Handbook of Applied Cryptography.* CRC Press, 1996. https://cacr.uwaterloo.ca/hac/

ISSN 3030-3907

4. Stallings, W. *Cryptography and Network Security: Principles and Practice.* 8th Edition, Pearson, 2020.
5. De Canniere, C., & Preneel, B. "Trivium Specifications." *eSTREAM Project Report*, 2005.
6. Hell, M., Johansson, T., & Meier, W. "Grain - a stream cipher for constrained environments." *International Journal of Wireless and Mobile Computing*, 2(1), 86–93 (2007).
7. Bernstein, D. J. "The Salsa20 family of stream ciphers." *New Stream Cipher Designs*, Springer, 2008

ISSN 3030-3907