KIMYO INTERNATIONAL UNIVERSITY IN
CENTRAL ASIAN JOURNAL OF STEM
ISSN 2181-2934 http://stem.kiut.uz/

SUN'IY INTELLEKT YORDAMIDA KRIPTOTIZIMLARNI TAHLIL QILISH

Rahmatullayev Ilhom Raxmatullayevich[1,2]

[1]Raqamli texnologiyalar va sun'iy intellektni rivojlantirish ilmiy-tadqiqot instituti doktoranti

[2]Toshkent Kimyo xalqaro universiteti Samarqand filiali dotsenti

ilhom9001@gmail.com

https://doi.org/10.5281/zenodo.18334349

Annotatsiya: Ushbu maqolada tenglamalar sistemasini yechish uchun Bees algoritmi qo'llanilishi ko'rib chiqiladi. Tenglamalar sistemasi chiziqli yoki chiziqli bo'lmagan bo'lishi hamda turli sonli noma'lumlarni o'z ichiga olishi mumkin. Tenglamalar sistemasining amaliy qo'llanilishi sifatida, oqimli shifrlash tizimlariga ochiq matn hujumi (yoki uning bir qismi) yordamida kriptotahlil hujum algoritmlarini amalga oshirish mumkin.

Kalit so'zlar: *sun'iy intellect, kriptotahlil, oqimli shifr, Geffe generatori, chiziqli teskari aloqali siljish registri (LFSR),ochiq matn hujumi, simmetrik kriptosistemalar, psevdotasodifiy bitlar generatori,chiziqli bo'lmagan tenglamalar sistemasi, kalit qidiruv*.

I.KIRISH

Tadqiqotning amaliy misoli sifatida Geffe sistemasi (chiziqli bo'lmagan kombinatsion funksiyaga ega) tanlangan. Bu sistema oqim shifrlash tizimlarining modeli sifatida chiziqli teskari aloqali siljish registrlari to'plamiga asoslanadi. Bees algoritmining samaradorligi ushbu registrlarning chiqishidagi istalgan sonli o'zgaruvchilar uchun tenglamalar sistemasini yechish orqali baholanadi.

Dasturning amaliy qismi ikki bosqichga bo‘lingan, birinchi, taklif etilgan kriptosistema uchun tenglamalar sistemasini tuzish, ikkinchi, tenglamalar sistemasidagi o‘zgaruvchilarga hujum qilish – bu o‘zgaruvchlar bir vaqtning o‘zida birlashtirilgan chiziqli teskari aloqali siljish registrlarining boshlang‘ich kalit qiymatlarini ifodalaydi.

Kriptotahlil shifrlarni tahlil qilish usullarini o‘rganadigan fan hisoblanadi. Bu, muammoni aniqlash uchun mukammal tizimdir. Kriptografiyaning maqsadi esa, aksincha, tahlil qilish qiyin bo‘lgan tizimlarni yaratishdir [1]. Kriptosistemaga muvaffaqiyatli hujum qilish uchun, kriptotahlil ma’lum yondashuvlarga tayanishga majbur bo‘ladi. Bularga shifrlangan matnning bir qismini bilish, foydalanilgan tilning xarakterli xususiyatlarini bilish va ba’zi omad kabi omillar kiradi.

Kriptosistemalar shifrlash va deshifrlash jarayonlariga asoslangan tizimlardir. Sun’iy intellekt (SI) texnikalaridan biri bo‘lgan To‘daviy intellekt (TI) – bu markazlashtirilmagan tizimlardagi barcha kollektiv xatti-harakatlarni o‘rganishni o‘z ichiga oladi. Bunday TI tizimlari oddiy agentlar yoki individlardan tashkil topgan bir (yoki bir nechta) populyatsiyalar orqali amalga oshiriladi. Ushbu agentlar bir-biri bilan va atrof-muhit bilan mahalliy yoki global darajada o‘zaro ta’sirlashadi. Garchi zarralarning harakatini boshqaradigan markaziy boshqaruv bo‘lmasada, ular o‘rtasidagi mahalliy o‘zaro ta’sirlar ko‘pincha global naqshlarning paydo bo‘lishiga olib keladi. Tabiatda bunday tizimlarning ko‘p misollarini topish mumkin: asalarilar, qushlar suruvi, bakteriyalar, chumolilar koloniyalari, hayvonlar podasi va boshqalar. Asalarilar algoritmi (AA), Chumoli koloniyasi optimizatsiyasi (ChKO) va Zarracha to‘dasi optimizatsiyasi (ZTO) kabi to‘daga o‘xshash algoritmlar muhandislik, iqtisod va telekommunikatsiya sohalaridagi real dunyo optimallashtirish muammolarini muvaffaqiyatli hal qilish uchun qo‘llanilgan [2].

Ismoil K.Ali (2009) o‘z dissertatsiyasida [3] Zarracha to‘dasi optimizatsiyasini (ZTO) oddiy transpozitsiya va oddiy almashtirish shifrlarini buzish uchun yaxshi vosita ekanligini ko‘rsatdi. Buning uchun har bir zarrachaning mosligini (fitness) aniqlashda bigramma va trigrammalardan foydalanilgan.

Ahmed T. va boshq. (2014) [4] transpozitsiya shifrlari avtomatik kriptotahlili uchun takomillashtirilgan cuckoo qidiruv algoritmini taklif qildi. Bu qidiruv algoritmi populyatsiya satrlari o‘rtasidagi o‘xshashliklarni tahlil qilish orqali maxfiy shifrlash (deshifrlash) kalitini topish uchun xarajat funksiyasining global maksimumini hisoblashni cuckoo qidiruv bosqichlariga qo‘shish yo‘li bilan amalga oshiriladi.

Hameed F. A. (2017) o‘z dissertatsiyasida [5] “ZTO asosidagi kriptotahlil tizimi” deb nomlangan, oqim shifri kriptosistemalariga ehtimoliy ochiq matn hujumi yordamida hujum qiluvchi tizimni amalga oshirdi. Turli tadqiqot holatlarini – yagona chiziqli teskari aloqali siljish registri (CTASR), chiziqli kriptosistema va boshiq generatori (chiziqli bo‘lmagan kriptosistema sifatida) – tanlab, yaxshi kriptotahlil natijalariga erishdi.

II.Asosiy qism

Ushbu ishda chiziqli bo‘lmagan oqim shifri generatoriga Asalarilar algoritmi yordamida hujum qilinadi. Tadqiqot holati sifatida Geffe generatori tanlanadi. Hujum usuli Geffe generatorining chiziqli bo‘lmagan tenglamalar sistemasini yechishga asoslanadi. Natijalar Asalarilar algoritmining oqim shifri kriptotahlilidagi yaxshi imkoniyatlarini ko‘rsatadi.

Zamonaviy kriptosistemalar

Asosan ikkita asosiy turdagi kriptografik tizimlar (kriptosistemalar) mavjud: maxfiy kalitli va ochiq kalitli kriptosistemalar [6]. Avval, ba’zi muhim belgilarni aniq qilamiz:

- P – ochiq (oddiy) matn xabari, C – shifrlangan matn xabari.
- Kalit fazosi K: ma’lum bir alifboga tegishli satrlar (kalitlar) to‘plami bo‘lib, shifrlash kaliti (e_k) va deshifrlash kaliti (d_k) ni o‘z ichiga oladi.
- Shifrlash algoritmi (jarayoni) E: $Ee_k(P) = C$.
- Deshifrlash algoritmi (jarayoni) D: $Dd_k(C) = P$.
- E va D algoritmlari quyidagi xossaga ega bo‘lishi shart: $Dd_k(C) = Dd_k(Ee_k(P)) = P$.

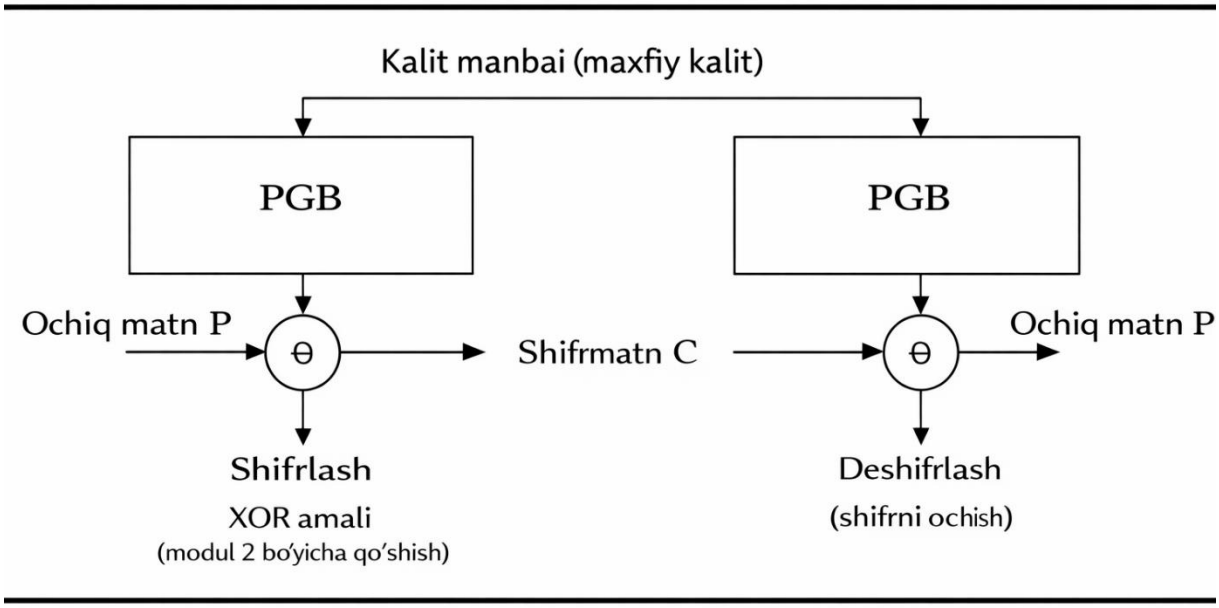
Ma’lumki, ochiq kalitli kriptosistema asimmetrik kriptosistemalar deb ham ataladi. Ochiq kalitli (maxfiy bo‘lmagan) kriptosistemada shifrlash kaliti (e_k) va deshifrlash kaliti (d_k) bir-biridan farq qiladi, ya’ni $e_k \neq d_k$.

Maxfiy kalitli kriptosistemalar esa simmetrik kriptosistemalar deb ham yuritiladi. Klassik maxfiy kalitli kriptosistemada shifrlash ham, deshifrlash ham uchun bir xil kalit ($e_k = d_k = k \in K$) ishlatiladi, bu kalit maxfiy kalit deyiladi. Bizning tadqiqotimizning maqsadi aynan shu turdagi kriptosistemalardir. Oqim shifri kriptosistemalari maxfiy kalitli kriptosistemalarning muhim turlaridan biridir [7].

Oqimli shifr tizimlari

Oqimli shifrlar kriptosistemalarning muhim sinflaridan biri hisoblanadi. Ular ochiq matn xabaridan bir vaqtning o‘zida olingan har bir raqamni (odatda ikkilik raqamlar) mustaqil ravishda shifrlaydi. Bunda vaqt o‘tishi bilan o‘zgarishi kerak bo‘lgan shifrlash funksiyasi yoki transformatsiyasidan foydalaniladi [8].

Oqim shifrlarida odatda xabarlarning birliklari bitlar (yoki raqamlar) bo‘ladi va kalit odatda psevdotasodifiy bitlar generatori (PTBG) deb ataladigan algoritm yordamida ishlab chiqariladi (1-rasmda ko‘rsatilganidek). Ochiq matn xabari bit-by-bit asosda amalga oshiriladigan usul bilan shifrlanadi.



1-rasm. Oqimli shifrlash kriptotizimining blok sxemasi.

Maxfiy kalit tasodifiy bitlar generatoriga kiritilib, uzun ikkilik signallar ketma-ketligini yaratadi. Ushbu kalit oqimi (k) odatda bit bo‘yicha modulo 2 qo‘shish (XOR) amali yordamida ochiq matn (p) bilan aralashtiriladi va shifrlangan matn oqimini hosil qilish uchun xuddi shu tasodifiy bitlar generatori va boshlang‘ich qiymat ishlatiladi.

Chiziqli teskari aloqali siljish registrlari (LFSR) kriptografiyada, ayniqsa oqim shifri kriptosistemalarida keng qo‘llaniladi. Har bir LFSR ikki asosiy qismdan iborat: mos boshlang‘ich holat qiymatlari bilan LFSR ulanish funksiyasi va ikkinchisi – kombinatsion funksiya (CF) bo‘lib, u mantiqiy (boolean) algebraik funksiya hisoblanadi. Aksariyat oqim shifrlari ana shu ikkita asosiy qismga tayanadi.

Amaliy oqimli shifrlarining aksariyati LFSR atrofida qurilgan. Elektronikaning zamonaviy tarixida ularni qurish juda oson edi. Siljish registrini bir qator bitli xotira hujayralari massivi deb ta’riflash mumkin, teskari aloqa ketma-ketliklari esa faqat XOR mantiqiy elementlari (logik darvozalar) qatoridan iborat. LFSR asosidagi oqimli shifrlar atigi bir nechta logik elementlar yordamida yuqori xavfsizlik va murakkablikni ta’minlay oladi [9], [10].

Tabiatdagi Asalarilar

Koloniyadagi har bir asalari o‘z-o‘zidan oziq-ovqat qidirishga kirishadi. Ma’lumki, asalarilar koloniyasi bir vaqtning o‘zida juda ko‘p sonli oziq-ovqat manbalaridan foydalanish uchun uzoq masofalarga va turli yo‘nalishlarda tarqalishi mumkin. Koloniya o‘zining oziq-ovqat yig‘uvchi asalarilarini mos dalalarga jo‘natish orqali rivojlanadi. Asosiy jihatdan, kamroq harakat bilan ko‘proq nektar yoki g‘ubor to‘plash mumkin bo‘lgan yaxshi gulli maydonlarga ko‘proq asalarilar tashrif buyurishi kerak, nektar yoki g‘ubori kam bo‘lgan maydonlarga esa kamroq asalarilar boradi. Oziq-ovqat yig‘ish jarayoni koloniyada “kashfiyotchi asalarilar” deb ataladigan asalarilarning istiqbolli gulli maydonlarni qidirish uchun yuborilishi bilan boshlanadi. Kashfiyotchi asalarilar bir maydondan ikkinchisiga tasodifiy harakat qiladi.

Yig‘im-terim mavsumi davomida koloniya o‘z izlanishlarini davom ettiradi va aholining ma’lum bir foizini kashfiyotchi asalarilar sifatida saqlaydi [11].

III. NATIJALAR

Asalarilar Algoritmi (BA)

Asalarilar jarayonining asosiy qiyinchiligi, muammolarni hal qilish uchun tanlangan koloniyaning o‘z-o‘zini tartibga solish xatti-harakatini moslashtirishdir [12]. Asalarilar Algoritmini asal asalarilarining tabiiy oziq-ovqat izlash xatti-harakatidan ilhomlangan va optimal yechimni topishga qaratilgan optimallashtirish algoritmi deb hisoblash mumkin.

Algoritm quyidagi parametrlarni sozlashni talab qiladi:

a. Kashfiyotchi asalarilar soni (n).

b. Tashrif buyurilgan "n" ta joydan tanlangan joylar soni (m).

c. Tanlangan "m" ta joy ichidagi eng yaxshi joylar soni (e).

d. Eng yaxshi "e" ta joy uchun jalb qilingan asalarilar soni (nep).

e. Qolgan (m – e) ta tanlangan joy uchun jalb qilingan asalarilar soni (nsp).

f. Maydonchalar (ngh)ning boshlang‘ich hajmi (o‘rni va uning atrofi) va to‘xtash mezonlari.

Eng sodda shakldagi Asalarilar algoritmining psevdokodi [13]:

Asalarilar Algoritmi

Kirish: (Kashfiyotchi asalarilar soni (n), tashrif buyurilgan "n" ta joydan tanlangan joylar soni (m), tanlangan "m" ta joy ichidagi eng yaxshi joylar soni (e), eng yaxshi "e" ta joy uchun jalb qilingan asalarilar soni (nep), qolgan (m-e) ta tanlangan joy uchun jalb qilingan asalarilar soni (nsp), maydonchalar (ngh)ning boshlang‘ich hajmi (o‘rni va uning atrofi), to‘xtash mezonlari, maksimal iteratsiyalar soni).

Chiqish: Optimal yechimlar.

1. Qadam: Populyatsiyani tasodifiy yechimlar bilan ishga tushirish.
2. Qadam: Populyatsiyaning mosligini (fitness) baholash.
3. Qadam: Takrorlash.
4. Qadam: Atrof-muhitni qidirish uchun joylarni tanlash.
5. Qadam: Tanlangan joylar uchun asalarilarni jalb qiling (eng yaxshi "e" ta joy uchun ko‘proq asalarilar) va ularning mosligini baholash.

6. Qadam: Har bir maydonchadan eng mos (fitness) asalarini tanlash.
7. Qadam: Qolgan asalarilarni yangi potentsial yechimlarni qidirish uchun kalit makonda tasodifiy tarqatish va ularning mosligini baholash.
8. Qadam: To‘xtash mezonlari qondirilmaguncha davom etish.

BA kalit qidiruv makonida tasodifiy tanlangan "n" ta kashfiyotchi asalari bilan boshlanadi. Kashfiyotchi asalarilar tashrif buyurgan joylarning moslik qiymatlari 2-qadamda baholanadi. 4-qadamda eng yaxshi moslikka ega bo‘lgan asalarilar "tanlangan asalarilar" deb tanlanadi va ular tashrif buyurgan joylar atrof-muhitni qidirish uchun belgilanadi. Keyin, 5 va 6-qadamlarda BA tanlangan joylarning atrofida qidiruv olib boradi, eng yaxshi "e" ta joylarga yaqinroq qidirish uchun ko‘proq asalarilarni tayinlaydi. Asalarilar ular tashrif buyurayotgan joylar bilan bog‘liq bo‘lgan yaxshi moslik qiymatlariga ko‘ra bevosita tanlanishi mumkin. Yoki, yuqori moslik qiymatlari asalarilarning tanlanish ehtimolini topish uchun ishlatiladi.

Eng istiqbolli yechimlarni ifodalovchi eng yaxshi "e" ta joylarning mahalliy yoki global atrofidagi qidiruvlar, boshqa tanlangan yaxshi asarilarga qaraganda ko‘proq asalarilarni jalb qilish orqali aniqroq amalga oshiriladi. Kashfiyotchilik bilan bir qatorda, bu farqli jalb qilish BA ning muhim asosiy operatsiyasidir.

Biroq, 6-qadamda har bir maydoncha uchun faqat eng yaxshi moslikka ega bo‘lgan asalari keyingi yaxshi asalar populyatsiyasini shakllantirish uchun tanlanadi. Tabiatda bunday cheklov mavjud emas. Bu cheklov bu yerda o‘rganilishi kerak bo‘lgan nuqtalar sonini kamaytirish uchun joriy qilingan.

7-qadamda populyatsiyadagi qolgan asalarilar yangi potentsial yechimlarni izlash uchun qidiruv makoni bo‘ylab tasodifiy tarqatilishi kerak. Ushbu qadamlarni to‘xtash mezonlari qondirilmaguncha takrorlash kerak. Qidiruv iteratsiyalari oxirida koloniyaning yangi populyatsiyasi ikkita qismdan iborat bo‘ladi: har bir tanlangan maydonchadan vakillar va tasodifiy qidiruv olib borish uchun tayinlangan boshqa kashfiyotchi asalarilar [14].

XULOSA

Mazkur maqolada sun’iy intellektga asoslangan optimallashtirish yondashuvlaridan biri bo‘lgan **Asalarilar algoritmi** yordamida **oqimli shifr kriptosistemalarini kriptotahlil qilish** masalasi tadqiq etildi. Tadqiqot doirasida chiziqli bo‘lmagan oqimli shifr generatori sifatida **Geffe generatori** tanlanib, unga nisbatan ochiq matn hujumi asosida kriptotahlil amalga oshirildi. Ushbu hujum generatorning chiziqli bo‘lmagan tenglamalar sistemasini tuzish va uni samarali yechish orqali boshlang‘ich kalit qiymatlarini aniqlashga qaratildi.

Olib borilgan tajribalar natijalari Asalarilar algoritmining katta o‘lchamli va murakkab kalit qidiruv makonlarida yuqori samaradorlikka ega ekanligini ko‘rsatdi. Algoritmning global va lokal qidiruv imkoniyatlarini uyg‘unlashtirishi hisobiga kalitlarni topish jarayoni an’anaviy deterministik usullarga nisbatan tezroq va ishonchliroq amalga oshirildi. Bu esa to‘daviy intellekt yondashuvlarining kriptotahlil sohasida qo‘llash imkoniyatlari keng ekanligini tasdiqlaydi.

Foydalanilgan adabiyotlar

[1] P. Ekdahl, *On LFSR Based Stream Ciphers Analysis and Design*, Ph.D. dissertation, Dept. of Economics, West Virginia University, Morgantown, WV, USA, Nov. 2003.

[2] Y. Liu and K. M. Passino, *Swarm Intelligence: Literature Overview*, Dept. of Electrical Engineering, The Ohio State University, Columbus, OH, USA, Mar. 30, 2000.

[3] I. K. Ali, *Intelligent Cryptanalysis Tool Using Particle Swarm Optimization*, Ph.D. dissertation, Dept. of Computer Science, University of Technology, Baghdad, Iraq, 2009.

[4] T. Ahmed, A. Laith, and K. Hashim, “Attacking transposition cipher using improved cuckoo search,” *Journal of Advanced Computer Science and Technology Research*, vol. 4, no. 1, pp. 22–32, Mar. 2014.

[5] F. A. Hameed, *Using Swarm Intelligence in Cryptanalysis of Nonlinear Stream Cipher Cryptosystem*, M.Sc. thesis, Dept. of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq, 2017.

[6] S. Y. Yan, *Number Theory for Computing*. Berlin, Germany: Springer-Verlag, 2000.

[7] B. Schneier, *Applied Cryptography*. New York, NY, USA: John Wiley & Sons, 1997.

[8] M. S. Mohammed, M. G. S. Al-Safi, and F. H. A., “Dynamic stream ciphering algorithm,” *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 2, ver. VIII, pp. 72–78, Mar.–Apr. 2014.

[9] J. Gu, X. Li, and Y. Hu, “Fault attack on the balanced shrinking generator,” *Wuhan University Journal of Natural Science*, vol. 11, no. 6, pp. 1773–1776, 2006.

[10] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA, USA: Holden-Day, 1967; reprinted by Aegean Park Press, 1982.

[11] M. Ibrahim, H. Rathiah, and E. A. Noor, "An overview of particle swarm optimization variants," *Procedia Engineering*, vol. 53, pp. 491–496, 2013.

[12] C. Chong, M. Y. H. Low, A. Sivakumar, and K. Gay, "A bee colony optimization algorithm to job shop scheduling," in *Proc. Winter Simulation Conf. (WSC)*, New Jersey, USA, 2006, pp. 1954–1960.

[13] A. Ashraf, P. Michael, and C. Marco, *Bees Algorithm*. Manufacturing Engineering Centre, Cardiff University, Wales, UK, 2009.

[14] D. T. Pham, A. Ghanbarzadeh, E. Koc, S. Otri, and M. Zaidi, "The bee's algorithm—A novel tool for complex optimization problems," in *Proc. 2nd Virtual Int. Conf. on Intelligent Production Machines and Systems*, D. T. Pham, E. Eldukhri, and A. J. Soroka, Eds. Oxford, UK: Elsevier, 2006, pp. 454–459.