# GIPERPARAMETRLARNI OPTIMALLASHTIRISH ASOSIDA SODDALASHTIRILGAN AES KALITLARINI TASNIFLASH USULI

Davlatov Mirzo-Ulug‘bek Bobir o‘g‘li
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti*
*mirzoulugbekdavlatov@gmail.com*

***Annotatsiya.*** *Maqolada Soddalashtirilgan AES (S-AES) algoritmi kalit bitlarini ochiqmatn–shifrmatn juftliklari asosida sun’iy neyron tarmoq yordamida tasniflashda model giperparametrlarini optimallashtirishga asoslangan usul taklif etiladi. 16 bitli ochiqmatn va unga mos 16 bitli shifrmatn birlashtirilib, 32 bitli kirish vektori shakllantiriladi, kalitning har bir biti alohida ikkilik tasniflash masalasi sifatida qaraladi. Neyron tarmoq arxitekturasi va o‘qitish giperparametrlarini avtomatik tanlash uchun genetik algoritmdan foydalanish nazarda tutiladi. Qidiruv jarayonida yashirin qatlamlar soni, neyronlar soni, faollashtirish funksiyasi, learning rate, batch size va Dropout kabi parametrlar baholanadi. Yondashuvning maqsadi yagona qo‘lda tanlangan konfiguratsiya o‘rniga kalit bitlarining xususiyatlariga mos konfiguratsiyalarni aniqlash va modelning umumlashtirish qobiliyatini oshirishdan iborat.*

***Kalit so‘zlar****: S-AES, sun’iy neyron tarmoq, giperparametr, genetik algoritm, kalit biti, ikkilik tasniflash, optimallashtirish, kriptotahlil.*

***Аннотация.*** *В статье предлагается метод классификации битов ключа упрощённого алгоритма AES (S-AES), основанный на оптимизации гиперпараметров искусственной нейронной сети по парам открытый текст–шифртекст. 16-битный открытый текст и соответствующий 16-битный шифртекст объединяются в 32-битный входной вектор, а каждый бит ключа рассматривается как отдельная задача бинарной классификации. Для автоматического выбора архитектуры сети и параметров обучения предлагается использовать генетический алгоритм. Оптимизируются число скрытых слоёв и нейронов, функция активации, скорость обучения, размер пакета и коэффициент Dropout. Цель подхода — подобрать конфигурации, соответствующие особенностям отдельных битов ключа, и повысить обобщающую способность модели.*

***Ключевые слова:*** *S-AES, искусственная нейронная сеть, гиперпараметры, генетический алгоритм, бит ключа, бинарная классификация, оптимизация, криптоанализ.*

***Abstract.*** *This article proposes a hyperparameter-optimization-based method for classifying individual key bits of the Simplified Advanced Encryption Standard (S-AES) using artificial neural networks and plaintext–ciphertext pairs. A 16-bit plaintext and its corresponding 16-bit ciphertext are concatenated into a 32-bit input vector, while each key bit is treated as an independent binary classification target. A genetic algorithm is used to search for suitable neural-network architectures and training hyperparameters, including hidden layers, neurons, activation function, learning rate, batch size and dropout rate. The method is intended to replace a single manually selected configuration with bit-specific optimized configurations and to improve generalization.*

***Keywords:*** *S-AES, artificial neural network, hyperparameter optimization, genetic algorithm, key bit, binary classification, cryptanalysis.*

**Kirish**

Raqamli axborot hajmining ortishi, bulutli hisoblash, mobil servislar va taqsimlangan axborot tizimlarining kengayishi ma’lumotlarning maxfiyligi, yaxlitligi va autentikligini ta’minlash masalasini yanada dolzarb qilmoqda. Simmetrik blokli shifrlash algoritmlari katta hajmdagi ma’lumotlarni tezkor himoyalashda muhim o‘rin tutadi. Advanced Encryption Standard (AES) zamonaviy simmetrik blokli shifrlash standartlaridan biri bo‘lib, NISTning FIPS 197 hujjatida AES-128, AES-192 va AES-256 variantlari 128 bitli bloklar bilan ishlashi belgilangan [3].

O‘zbekistonda sun’iy intellekt va kiberxavfsizlik yo‘nalishlarining rivojlantirilishi zamonaviy hisoblash usullarini axborot xavfsizligi masalalariga tatbiq etish bo‘yicha ilmiy tadqiqotlarning ahamiyatini oshirmoqda. 2024-yil 14-oktabrdagi PQ-358-son qaror bilan sun’iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi tasdiqlangan [1]. 2026-yil 10-martdagi PF-38-son Farmonda esa kiberxavfsizlikni kuchaytirish, axborot tizimlari va muhim axborot infratuzilmasini himoyalash vazifalari belgilangan [2].

Kriptotahlilda an’anaviy differensial va chiziqli yondashuvlar bilan bir qatorda mashinali o‘qitish va chuqur o‘qitish usullaridan foydalanish ham tadqiq qilinmoqda. Bunday modellar ochiqmatn, shifrmatn va kalit o‘rtasidagi murakkab nochiziqli munosabatlardan statistik belgilarni ajratishga urinadi. Shu bilan birga, o‘quv tanlanmasidagi yuqori aniqlikning o‘zi kriptografik zaiflikni

isbotlamaydi. Mustaqil nazorat natijasi, tasodifiy bazaviy daraja va modelning umumlashtirish qobiliyati alohida baholanishi lozim [5, 6].

To‘liq AESni sun’iy neyron tarmoq yordamida bevosita buzish ushbu tadqiqotning maqsadi emas. Eksperimental muhit sifatida Musa, Schaefer va Wedig tomonidan taklif qilingan S-AES tanlangan. S-AES AESning asosiy strukturaviy g‘oyalarini kichik o‘lchamda ifodalaydi hamda chiziqli va differensial kriptotahlil tajribalarini tushuntirish uchun ishlab chiqilgan [4]. Shu sababli u neyron tarmoq asosidagi kalit bitlarini tasniflash usullarini nazorat qilinadigan sharoitda tekshirish uchun qulay modeldir.

Muallifning oldingi tajribalarida 16 bitli ochiqmatn va 16 bitli shifrmatn birlashtirilib, 32 bitli kirish vektori shakllantirilgan hamda 16 bitli shifr kalitining har bir biti alohida ikkilik tasniflash vazifasi sifatida qaralgan. Sinovdan o‘tkazilgan konfiguratsiyalar orasida GeLU va Binary Crossentropy kombinatsiyasi 0,9750 o‘quv va 0,5750 nazorat aniqligini ko‘rsatgan. Natijalar model konfiguratsiyasi muhimligini, lekin overfitting muammosi mavjudligini ko‘rsatadi.

Ayrim kalit bitlarida nazorat aniqligining 0,60–0,61 gacha yetishi, boshqa bitlarda esa 0,50 ga yaqin qolishi barcha bitlar uchun yagona arxitektura va bir xil giperparametrlar optimal bo‘lmasligi mumkinligini ko‘rsatadi. Mazkur maqolada shu muammo keyingi bosqichga olib chiqilib, S-AES kalit bitlarini tasniflashda giperparametrlarni genetik algoritm yordamida avtomatik optimallashtirish usuli ishlab chiqiladi.

Tadqiqotning maqsadi S-AES ochiqmatn–shifrmatn juftliklari asosida kalit bitlarini tasniflovchi sun’iy neyron tarmoq uchun arxitektura va o‘qitish giperparametrlarini avtomatik tanlash usulini shakllantirish, bitga mos konfiguratsiyalarni aniqlash hamda modelni mustaqil test ma’lumotlarida baholash metodologiyasini taklif etishdan iborat.

**Mavzuga oid adabiyotlar sharhi**

AES algoritmining standart va nazariy asoslari NIST FIPS 197 hujjatida bayon qilingan. 2023-yilda yangilangan nashr algoritmning texnik mohiyatini o‘zgartirmagan holda atamalar, belgilar va kalitlar jadvali bo‘yicha tushuntirishlarni takomillashtirdi [3]. AESning rivojlanish tarixi bo‘yicha NIST tadqiqotlarida kuchli blokli shifrlarning saqlanayotgan va uzatilayotgan ma’lumotlarni himoyalashdagi fundamental o‘rni qayd etilgan [7].

S-AES algoritmi Musa, Schaefer va Wedig tomonidan AESning ishlash tamoyillarini kichik o‘lchamda tushuntirish va kriptotahlil tajribalarini o‘tkazish uchun taklif qilingan [4]. Soddalashtirilgan kalit va blok o‘lchamlari S-AESni

yangi tahlil metodlarini dastlabki bosqichda sinash uchun qulay eksperimental obyektga aylantiradi. Biroq S-AESda olingan natijalarni standart AES xavfsizligiga bevosita ko‘chirish metodologik jihatdan to‘g‘ri emas.

Brunetta va Picazo-Sanchez mashinali o‘qitish yordamida kriptografik farqlovchilarni modellashtirish imkoniyatlarini o‘rganib, tajriba modeli va hujum shartlarini aniq ifodalash zarurligini ko‘rsatadi [5]. Neyron model o‘quv ma’lumotlaridagi takroriy yoki tasodifiy xususiyatlarni ham yodlab olishi mumkin. Shu sababli train, validation va test tanlanmalarining mustaqilligi kriptografik ML tajribalarida alohida ahamiyatga ega.

2023-yilda lightweight blokli shifrlar bo‘yicha e’lon qilingan tadqiqotda S-DES, S-AES va S-SPECK uchun chuqur o‘qitishga asoslangan kalitni tiklash yondashuvlari qayta ko‘rib chiqilgan [6]. Zamonaviy arxitektura elementlari ayrim vazifalarda natijani yaxshilashi mumkinligi ko‘rsatilgan bo‘lsa-da, to‘liq raund va to‘liq kalitli zamonaviy shifrlar uchun amaliy kalit tiklash juda murakkabligicha qolishi ta’kidlangan.

2024-yildagi kompleks neyron kriptotahlil tadqiqotida DES, S-DES, AES, S-AES va SPECK turli vazifalar bo‘yicha tahlil qilingan [8]. Natijalar shifr turi, raundlar soni, ma’lumot hajmi va neyron arxitektura yakuniy samaradorlikka bevosita ta’sir qilishini ko‘rsatadi. Shifrlashni emulyatsiya qilish, ochiqmatnni tiklash, kalitni tiklash va shifrmatnni tasniflash bir xil masala emasligi ham metodologik jihatdan muhimdir.

Sun’iy neyron tarmoqda giperparametrlar model o‘qitilishidan oldin belgilanadigan boshqaruv parametrlaridir. Yashirin qatlamlar soni, har bir qatlamdagi neyronlar, faollashtirish funksiyasi, learning rate, batch size va muntazamlashtirish darajasi modelning o‘rganish tezligi, sig‘imi va umumlashtirish qobiliyatiga ta’sir qiladi. Giperparametrlarning noto‘g‘ri tanlanishi underfitting yoki overfittingga olib kelishi mumkin.

Giperparametrlarni qo‘lda tanlash tajribachi qaroriga kuchli bog‘liq. Grid Search barcha belgilangan kombinatsiyalarni tekshirishi mumkin, biroq parametrlar soni va ularning qiymatlari ortgan sari qidiruv maydoni keskin kengayadi. Random Search ayrim holatlarda samaraliroq bo‘lsa-da, avvalgi muvaffaqiyatli kombinatsiyalar xususiyatlaridan yangi kandidatlarni yaratish mexanizmiga ega emas.

Genetik algoritm evolyutsion optimallashtirish paradigmasiga mansub bo‘lib, potensial yechimlar populyatsiyasini selection, crossover va mutation operatorlari yordamida bosqichma-bosqich takomillashtiradi [9]. Neyron tarmoq giperparametrlarini optimallashtirishda har bir individ ma’lum arxitektura va

o‘qitish sozlamalarini kodlashi mumkin. Fitness funksiyasi esa kandidat konfiguratsiyaning validation ma’lumotlaridagi sifatini ifodalaydi.

Mazkur maqolaning ilmiy yondashuvi kalitning 16 bitini bitta ko‘p sinfli vazifa sifatida emas, 16 ta alohida ikkilik tasniflash masalasi sifatida qarash va har bir bit uchun giperparametrlarni alohida qidirishdan iborat. Bu yondashuv oldingi tajribalarda kuzatilgan bitlar kesimidagi notekis natijalarni hisobga olish imkonini beradi.

**Tadqiqot metodologiyasi**

Tadqiqot eksperimental yondashuv asosida tashkil etiladi. Dastlab S-AES algoritmi yordamida 16 bitli ochiqmatn P, 16 bitli kalit K va mos 16 bitli shifrmatn C dan iborat namunalar shakllantiriladi. Shifrlash jarayoni C = E_K(P) ko‘rinishida ifodalanadi. Ma’lumotlar generatsiyasida ochiqmatn va kalit qiymatlarining taqsimoti nazorat qilinishi, train va test namunalarining tasodifiy takrorlanishi oldi olinishi zarur.

Neyron tarmoq uchun kirish vektori ochiqmatn va shifrmatnni ketma-ket birlashtirish orqali hosil qilinadi: $X = P \| C$, $X \in \{0,1\}^{32}$. Natijada har bir kuzatuv 32 ta ikkilik belgidan tashkil topadi. Kalit $K = (k_1, k_2, \ldots, k_{16})$ ko‘rinishida bo‘lib, har bir $y_i = k_i$ alohida maqsadli o‘zgaruvchi sifatida belgilanadi. Shu tariqa 16 ta ikkilik tasniflash masalasi hosil bo‘ladi.

Tasniflash modeli sifatida ko‘p qatlamli perseptron qo‘llanadi. Umumiy qatlam $h^{(l)}=\varphi(W^{(l)}h^{(l-1)}+b^{(l)})$ ko‘rinishida ifodalanadi. Bu yerda W va b o‘qitish davomida gradient asosidagi optimizator orqali o‘rganiladigan model parametrlari, φ esa faollashtirish funksiyasidir. Ikkilik chiqish uchun sigmoid va Binary Crossentropy metodologik jihatdan tabiiy tanlov hisoblanadi.

Model parametrlari bilan giperparametrlarni farqlash zarur. Weight va bias qiymatlari backpropagation orqali o‘rganiladi; yashirin qatlamlar soni, neyronlar soni, faollashtirish funksiyasi, learning rate, batch size, Dropout va o‘qitish chegaralari esa giperparametrlar hisoblanadi. Ushbu maqolada aynan ikkinchi guruhni avtomatik qidirish asosiy masala sifatida qaraladi.

Giperparametrlar to‘plami $H=\{L,N_1,\ldots,N_L,A,\eta,B,D\}$ bilan belgilanadi. Bu yerda L — yashirin qatlamlar soni, N — qatlamdagi neyronlar soni, A — faollashtirish funksiyasi, η — learning rate, B — batch size, D — Dropout koeffitsiyenti. Qidiruv fazosi oldindan amaliy diapazonlar bilan chegaralanadi, chunki cheksiz qidiruv hisoblash xarajatlarini oshiradi.

Genetik algoritmning boshlang‘ich bosqichida $Population_0=\{H_1,H_2,\ldots,H_n\}$ ko‘rinishidagi kandidat konfiguratsiyalar yaratiladi. Har bir individ bitta to‘liq SNT konfiguratsiyasini ifodalaydi. Masalan, ikki yashirin qatlam, 128 va 64

neyron, GeLU, learning rate 0,001, batch size 32 va Dropout 0,2 qiymatlari bitta individning genlari sifatida qaralishi mumkin.

Har bir kandidat model bir xil training ma'lumotlarida o'qitiladi va validation to'plamida baholanadi. Fitness(H_j)=ValidationScore(H_j) asosiy ko'rinish bo'lsa-da, faqat accuracydan foydalanish har doim yetarli emas. Sinflar balanssiz bo'lsa F1-score yoki balanced accuracy maqsadga muvofiq. Bundan tashqari, train-validation tafovutini jarimaga kiritish overfittingga moyil konfiguratsiyalarning tanlanishini kamaytirishi mumkin.

Selection bosqichida fitness qiymati yuqori individlar keyingi avlod uchun ota-ona sifatida tanlanadi. Crossover ikki konfiguratsiyaning ayrim genlarini birlashtirib yangi kandidat yaratadi. Masalan, birinchi ota-onadan faollashtirish funksiyasi va batch size, ikkinchisidan qatlam tuzilishi va learning rate olinishi mumkin. Mutation esa qidiruv xilma-xilligini saqlash uchun ayrim genlarni belgilangan ehtimollik bilan o'zgartiradi.

Genetik algoritmda crossover va mutation optimallashtirish operatorlari hisoblanadi. EarlyStopping va ModelCheckpoint esa genetik operatorlar emas. EarlyStopping validation ko'rsatkichi ma'lum muddat yaxshilanmasa o'qitishni to'xtatadi, ModelCheckpoint esa o'qitish jarayonidagi eng yaxshi model holatini saqlaydi. Ular har bir individni baholash xarajatini kamaytirish va ortiqcha o'qitishni nazorat qilish uchun qo'llanadi.

Taklif etilayotgan bitga mos optimallashtirishda har bir $k_i$ uchun $H_i^*$ = argmax_H Fitness(H,$k_i$) topiladi. Natijada $k_1 \rightarrow H_1^*$, $k_2 \rightarrow H_2^*$, …, $k_{16} \rightarrow H_{16}^*$ mosliklari hosil bo'ladi. Bu barcha bitlarga bitta arxitekturani majburan qo'llash o'rniga har bir tasniflash vazifasining statistik xususiyatiga mos konfiguratsiyani tanlash imkonini beradi.

Ma'lumotlarni Training–Validation–Final Test ko'rinishida uch qismga ajratish taklif etiladi. Training to'plami weight va biaslarni o'rganish uchun, validation to'plami GA fitnessini hisoblash va giperparametr tanlash uchun ishlatiladi. Final test to'plami esa GA qidiruvida umuman qatnashmaydi. Bu validation to'plamiga ortiqcha moslashish natijasini yakuniy samaradorlik sifatida noto'g'ri talqin qilish xavfini kamaytiradi.

Yakuniy baholashda accuracy bilan cheklanmasdan precision, recall, F1-score va ROC-AUC ko'rsatkichlari hisoblanishi kerak. Bir xil konfiguratsiyani bir necha random seed bilan qayta o'qitish, o'rtacha qiymat va standart og'ishni keltirish tasodifiy boshlang'ich vaznlar ta'sirini baholashga yordam beradi. Optimallashtirishdan oldingi va keyingi modellar aynan bir xil test to'plamida solishtirilishi zarur.

**Tahlil va natijalar**

Dastlabki bosqichda giperparametrlarni avtomatik optimallashtirishdan oldingi MLP konfiguratsiyalarining natijalari tayanch nuqta sifatida olinadi. Ushbu natijalar model arxitekturasi va o‘qitish sozlamalari tasniflash samaradorligiga ta’sir qilishini ko‘rsatgan. Shu bilan birga, yuqori training accuracy mustaqil ma’lumotlardagi yuqori aniqlikni kafolatlamagan.

**1-jadval. MLP konfiguratsiyalarining S-AES kalit bitlarini tasniflash natijalari**

| Model | Faollashtirish | Yo‘qotish funksiyasi | O‘quv aniqligi | Nazorat aniqligi |
|---|---|---|---|---|
| MLP 1 | Softmax | MSE | 0,5012 | 0,5120 |
| MLP 2 | ReLU | MAE | 0,4988 | 0,4880 |
| MLP 3 | ReLU | Binary Crossentropy | 0,9120 | 0,5330 |
| MLP 4 | ReLU | Cosine Similarity | 0,5012 | 0,5120 |
| MLP 5 | ReLU | MSE | 0,9280 | 0,5210 |
| MLP 6 | PReLU | Binary Crossentropy | 0,8271 | 0,5135 |
| MLP 7 | GeLU | Binary Crossentropy | 0,9750 | 0,5750 |
| MLP 8 | Swish | Binary Crossentropy | 0,6862 | 0,5125 |
| MLP 9 | Sigmoid | MSE | 0,5041 | 0,4880 |

*Manba: muallifning dissertatsiya doirasidagi tajriba natijalari asosida tuzilgan.*

1-jadvaldan ko‘rinadiki, Softmax–MSE, ReLU–MAE, ReLU–Cosine Similarity va Sigmoid–MSE konfiguratsiyalari 0,50 atrofidagi natijalarni qayd etgan. Ikkilik tasniflashda bu qiymat tasodifiy taxmin darajasiga yaqin. Demak, mazkur konfiguratsiyalarda model kalit bitiga oid barqaror ajratuvchi signalni umumlashtira olmagan.

ReLU–Binary Crossentropy konfiguratsiyasida o‘quv aniqligi 0,9120 bo‘lsa, nazorat aniqligi 0,5330 ni tashkil etgan. ReLU–MSE konfiguratsiyasida training accuracy 0,9280 gacha ko‘tarilgan, ammo validation natijasi 0,5210 bo‘lgan. Bu holatlar yuqori o‘quv aniqligi mustaqil ma’lumotlardagi samaradorlikni ifodalamasligini yana bir bor ko‘rsatadi.

Eng yuqori dastlabki nazorat natijasi GeLU–Binary Crossentropy konfiguratsiyasida kuzatilgan: o‘quv aniqligi 0,9750, nazorat aniqligi 0,5750. Ular orasidagi 0,4000 tafovut kuchli overfitting belgisi hisoblanadi. Shuning

uchun 97,5 foizlik training natijasini kalit biti 97,5 foiz aniqlikda tiklandi deb talqin qilish ilmiy jihatdan asosli emas.

Oldingi tajribalarda namunalar sonini 500 tadan 20 000 tagacha oshirish ayrim konfiguratsiyalarda o‘quv aniqligini juda yuqori qiymatlarga olib kelgan bo‘lsa-da, nazorat natijalari barqaror oshmagan. Bu muammo faqat ma’lumotlar hajmiga bog‘liq emasligini, model sig‘imi, regularizatsiya, learning rate, batch size va boshqa giperparametrlarning o‘zaro ta’siri mavjudligini ko‘rsatadi.

Bitlar kesimidagi natijalar ham bir xil bo‘lmagan. Ayrim kalit bitlarida nazorat aniqligi 0,60–0,61 oralig‘iga chiqqan, boshqa bitlarda esa 0,50 atrofida qolgan. Ushbu kuzatuv taklif etilayotgan bitga mos giperparametr optimallashtirishning asosiy eksperimental motivatsiyasini tashkil etadi.

Taklif etilgan GA yondashuvida optimallashtirish natijasi oldingi MLP 7 ko‘rsatkichi bilan bir xil final test to‘plamida solishtirilishi kerak. Bunda yangi modelning faqat training natijasi emas, validation va final test ko‘rsatkichlari, train-test tafovuti hamda bir necha ishga tushirish bo‘yicha barqarorligi hisobga olinadi.

Optimallashtirishning asosiy kutiladigan amaliy natijasi barcha bitlar uchun bitta universal konfiguratsiyani qidirish emas, balki qaysi bitlar uchun qanday arxitektura va o‘qitish parametrlarining samaraliroq ekanini aniqlashdir. Masalan, bir bit uchun kichikroq tarmoq va yuqoriroq Dropout optimal bo‘lishi, boshqa bit uchun chuqurroq tarmoq va kichik learning rate talab qilinishi mumkin. Bunday farq faqat eksperimental qidiruv natijasida tasdiqlanishi kerak.

Fitness funksiyasini shakllantirishda faqat validation accuracydan foydalanish sodda va tushunarli, ammo u har doim yetarli emas. Agar sinflar taqsimoti nomutanosib bo‘lsa, balanced accuracy yoki F1-score qo‘llanishi mumkin. Bundan tashqari, Fitness = ValidationScore − $\lambda|\text{TrainScore}-\text{ValidationScore}|$ ko‘rinishidagi jarimali mezon overfittingga moyil konfiguratsiyalarni pastroq baholash imkonini beradi. $\lambda$ koeffitsiyenti tajriba orqali belgilanadi.

Genetik algoritm hisoblash xarajatini ham yuzaga keltiradi, chunki har bir avloddagi har bir individ uchun alohida SNT o‘qitiladi. Shu sababli populyatsiya hajmi, avlodlar soni va qidiruv diapazonlari hisoblash resurslariga mos tanlanishi lozim. EarlyStopping muvaffaqiyatsiz kandidatlarni erta to‘xtatish orqali qidiruv vaqtini qisqartirishga yordam beradi.

Optimallashtirish jarayonining ilmiy ishonchliligi uchun test to‘plamini GA qidiruvidan qat’iy ajratish zarur. Aks holda test natijasi ham bilvosita giperparametr tanlashga ta’sir qilib, yakuniy bahoning optimistik chiqishiga olib

keladi. Shu sababli final test faqat barcha giperparametrlar tanlanganidan keyin bir marta yoki oldindan belgilangan protokol asosida qo‘llanishi kerak.

Taklif etilgan metodni amaliy kriptotahlil vositasi sifatida emas, balki S-AES muhitida neyron tarmoqning kalit bitlariga oid statistik signalni ajratish qobiliyatini o‘rganish metodologiyasi sifatida talqin qilish lozim. S-AESda olingan natijalar to‘liq AES xavfsizligi buzilganini anglatmaydi. Keyingi tadqiqotlarda raundlar va kalit murakkabligi bosqichma-bosqich oshirilib, metodning chegaralari tekshirilishi mumkin.

Taklif etilgan usulning ilmiy yangilik elementi S-AES kalit bitlarini tasniflashda neyron tarmoq arxitekturasi va o‘qitish giperparametrlarini oldindan bitta qat’iy konfiguratsiya sifatida belgilashdan voz kechib, ularni genetik algoritm orqali bitlar kesimida optimallashtirish konsepsiyasini shakllantirishdan iborat. Bunda optimallashtirishning natijasi mustaqil test tanlanmasida tekshirilishi metodning ajralmas qismi sifatida qaraladi.

**Xulosa va takliflar**

1. S-AES algoritmida 16 bitli ochiqmatn va 16 bitli shifrmatndan hosil qilingan 32 bitli kirish vektori kalitning individual bitlarini alohida ikkilik tasniflash vazifasi sifatida ifodalash uchun metodik asos yaratadi.

2. Dastlabki MLP tajribalari model konfiguratsiyasi natijaga sezilarli ta’sir qilishini ko‘rsatdi. GeLU va Binary Crossentropy kombinatsiyasida 0,9750 training va 0,5750 validation aniqligi kuzatilgani yuqori o‘quv natijasining o‘zi umumlashtirishni kafolatlamasligini ko‘rsatadi.

3. Kalit bitlari bo‘yicha natijalarning farqlanishi barcha bitlarga yagona konfiguratsiya qo‘llash o‘rniga bitga mos arxitektura va giperparametrlarni izlash zaruratini yuzaga keltiradi.

4. Giperparametrlarni avtomatik tanlash uchun genetik algoritmdan foydalanish taklif etildi. Qidiruv fazosiga yashirin qatlamlar, neyronlar soni, faollashtirish funksiyasi, learning rate, batch size va Dropout kiritiladi.

5. Selection, crossover va mutation genetik algoritmning asosiy optimallashtirish operatorlaridir. EarlyStopping va ModelCheckpoint esa har bir kandidat SNTni o‘qitishni nazorat qiluvchi yordamchi mexanizmlar sifatida qo‘llanishi kerak.

6. Giperparametrlarni tanlash validation to‘plamida amalga oshirilishi, final test esa optimallashtirish jarayonidan butunlay ajratilishi zarur. Bu metod samaradorligini xolis baholash uchun muhim.

7. Yakuniy baholashda accuracy bilan bir qatorda precision, recall, F1-score, ROC-AUC, o‘rtacha qiymat va standart og‘ish kabi ko‘rsatkichlardan foydalanish tavsiya etiladi.

8. Optimallashtirishdan oldingi va keyingi modellar bir xil ma’lumot ajratilishi, bir xil final test to‘plami va bir xil baholash mezonlarida solishtirilishi kerak. Aks holda natijadagi farqni faqat GA optimallashtirishiga bog‘lash mumkin bo‘lmaydi.

9. Taklif etilgan usulning ilmiy yangiligi S-AES kalit bitlarini tasniflashda har bir bit uchun sun’iy neyron tarmoq arxitekturasi va o‘qitish giperparametrlarini genetik algoritm asosida moslashtirish hamda ularni mustaqil test to‘plamida tekshirishga asoslangan metodologik yondashuvdan iborat.

10. Olingan natijalar standart AES xavfsizligi buzilganini anglatmaydi. Kelgusida raundlar soni va kalit murakkabligini bosqichma-bosqich oshirish, boshqa soddalashtirilgan blokli shifrlar bilan qiyoslash hamda optimallashtirish xarajatlarini tahlil qilish taklif etiladi.

**Foydalanilgan adabiyotlar**

1. O‘zbekiston Respublikasi Prezidenti. Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida: PQ-358-son qaror. — 2024-yil 14-oktabr. — Qonunchilik ma’lumotlari milliy bazasi — LexUZ.

2. O‘zbekiston Respublikasi Prezidenti. O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida: PF-38-son Farmon. — 2026-yil 10-mart. — Qonunchilik ma’lumotlari milliy bazasi — LexUZ.

3. National Institute of Standards and Technology. Advanced Encryption Standard (AES): FIPS PUB 197-upd1. — U.S. Department of Commerce, 2023. DOI: 10.6028/NIST.FIPS.197-upd1.

4. Musa M. A., Schaefer E. F., Wedig S. A simplified AES algorithm and its linear and differential cryptanalyses // Cryptologia. — 2003. — Vol. 27, № 2. — P. 148–177. DOI: 10.1080/0161-110391891838.

5. Brunetta C., Picazo-Sanchez P. Modelling cryptographic distinguishers using machine learning // Journal of Cryptographic Engineering. — 2022. — Vol. 12. — P. 123–135. DOI: 10.1007/s13389-021-00262-x.

6. Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited // Entropy. — 2023. — Vol. 25, № 7. — 986. DOI: 10.3390/e25070986.

7. Smid M. E. Development of the Advanced Encryption Standard // Journal of Research of the National Institute of Standards and Technology. — 2021. — Vol. 126. — 126024. DOI: 10.6028/jres.126.024.

8. Comprehensive Neural Cryptanalysis on Block Ciphers Using Different Encryption Methods // Mathematics. — 2024. — Vol. 12, № 13. — 1936. DOI: 10.3390/math12131936.

9. Holland J. H. Adaptation in Natural and Artificial Systems. — University of Michigan Press, 1975.