KRIPTOGRAFIYA VA KRIPTOTAHLIL MASALALARIDA SUN’IY NEYRON TARMOQLARDAN FOYDALANISH

Davlatov Mirzo-Ulug‘bek Bobir o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti tayanch doktoranti
ORCID: 0009-0003-5246-9521;
e-mail: mirzoulugbekdavlatov@gmail.com

Annotatsiya*. Ushbu maqolada sun’iy neyron tarmoqlarning kriptografiya va kriptotahlil masalalaridagi o‘rni, ularning kriptografik ma’lumotlardagi murakkab nolinear bog‘lanishlarni o‘rganish qobiliyati hamda blokli shifrlar, neyron distinguisherlar, kalit bitlarini tasniflash va yon kanal tahlilidagi imkoniyatlari ko‘rib chiqiladi. An’anaviy statistik kriptotahlil bilan neyron yondashuvning o‘zaro to‘ldiruvchi jihatlari tahlil qilinadi. AES misolida neyron tarmoqlardan foydalanishning istiqbollari, cheklovlari va eksperimental baholash mezonlari yoritiladi.*

Kalit so‘zlar: *sun’iy neyron tarmoq, kriptografiya, kriptotahlil, AES, chuqur o‘rganish, neyron distinguisher, kalit tasnifi, yon kanal hujumi.*

Аннотация. *В статье рассматривается роль искусственных нейронных сетей в задачах криптографии и криптоанализа, их способность выявлять сложные нелинейные зависимости в криптографических данных, а также возможности применения для блочных шифров, нейронных различителей, классификации битов ключа и анализа побочных каналов. Анализируются взаимодополняющие стороны традиционного статистического криптоанализа и нейросетевого подхода. На примере AES показаны перспективы, ограничения и критерии экспериментальной оценки нейросетевых методов.*

Ключевые слова*: искусственная нейронная сеть, криптография, криптоанализ, AES, глубокое обучение, нейронный различитель, классификация ключа, атака по побочным каналам.*

Abstract*. This article examines the role of artificial neural networks in cryptography and cryptanalysis, focusing on their ability to learn complex nonlinear dependencies in cryptographic data and their use in block-cipher analysis, neural distinguishers, key-bit classification, and side-channel analysis. The complementary relationship between traditional statistical cryptanalysis and neural approaches is*

discussed. Using AES as a representative case, the paper outlines promising applications, limitations, and experimental evaluation criteria for neural-network-based methods.

Keywords: *artificial neural network, cryptography, cryptanalysis, AES, deep learning, neural distinguisher, key classification, side-channel attack.*

KIRISH

Raqamli axborot almashinuvi hajmining ortishi ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlashga bo‘lgan talabni kuchaytirmoqda. Zamonaviy kriptografik algoritmlar ushbu vazifalarni matematik jihatdan asoslangan murakkab o‘zgartirishlar orqali bajaradi. Shu bilan birga, kriptotahlilning vazifasi shifr tuzilmasidagi statistik, algebraik yoki implementatsion zaifliklarni aniqlash va ularning amaliy xavfsizlikka ta’sirini baholashdan iborat. AES kabi standart blokli shifrlar to‘liq raundli konfiguratsiyada klassik differensial va chiziqli tahlilga nisbatan yuqori bardoshlilikka ega bo‘lsa-da, qisqartirilgan raundlar, noto‘g‘ri implementatsiya yoki yon kanal sizib chiqishlari ilmiy tahlil uchun muhim obyekt bo‘lib qolmoqda [1, 149–167-b.].

So‘nggi yillarda mashinaviy o‘qitish, ayniqsa sun’iy neyron tarmoqlar kriptotahlilda qo‘shimcha analitik vosita sifatida faol o‘rganilmoqda. Buning asosiy sababi neyron tarmoqlarning katta hajmdagi ma’lumotlarda oldindan aniq ifodalanmagan nolinear bog‘lanishlarni o‘rganish qobiliyatidir. Kriptografik ma’lumotlar ataylab tasodifiy ko‘rinishga keltirilgani sababli bunday vazifa oddiy klassifikatsiyadan ancha murakkabdir. Shunga qaramay, qisqartirilgan raundli ayrim shifrlarda neyron distinguisherlar klassik differensial distinguisherlardan kuchliroq belgilarni o‘rganishi mumkinligi ko‘rsatilgan [2, 1–3-b.].

Maqolaning maqsadi sun’iy neyron tarmoqlarning kriptografiya va kriptotahlildagi asosiy qo‘llanish yo‘nalishlarini tizimlashtirish, ularning blokli shifrlar va AES bilan bog‘liq tadqiqotlardagi imkoniyatlarini tahlil qilish hamda neyron tarmoqqa asoslangan eksperimental kriptotahlil uchun metodik ketma-ketlikni shakllantirishdan iborat. Tadqiqotda nazariy tahlil, qiyosiy tahlil, model abstraksiyasi va eksperimental dizayn usullaridan foydalaniladi.

MAVZUGA OID ADABIYOTLAR SHARHI

Sun’iy neyron tarmoqlarni kriptografiya va kriptotahlil masalalariga tatbiq etish bo‘yicha ilmiy izlanishlar so‘nggi yillarda alohida tadqiqot yo‘nalishiga aylandi. Xorijiy adabiyotlarda bu yo‘nalishning shakllanishida Aron Gohrning ishlari muhim o‘rin tutadi. A. Gohr 2019-yilda SPECK32/64 blokli shifrining qisqartirilgan raundlariga qarshi chuqur o‘rganishga asoslangan neyron

distinguisherni taklif qilib, residual neyron tarmoqlar shifrmatn juftliklaridagi klassik differensial tahlilda to‘liq ifodalanmaydigan belgilarni ham o‘rganishi mumkinligini ko‘rsatdi [2, 150–179-b.]. Mazkur ish neural differential cryptanalysis yo‘nalishining keyingi rivojlanishiga asos bo‘ldi.

Gohr yondashuvining ichki ishlash mexanizmini tushuntirishga qaratilgan tadqiqotlar ham olib borildi. Adrien Benamira, David Gérault, Thomas Peyrin va Quan Quan Tan neyron distinguisherlar qaysi kriptografik xususiyatlardan foydalanishini tahlil qilib, model differensial taqsimot jadvalidagi ma’lumotni o‘zlashtirish bilan birga undan tashqaridagi qo‘shimcha statistik belgilarni ham o‘rganishini ko‘rsatdilar [9]. Bu natija neyron tarmoqni shunchaki “qora quti” klassifikatori sifatida emas, balki differensial kriptotahlilni boyituvchi vosita sifatida o‘rganishga turtki berdi.

Jinyu Lu va hammualliflar neural-differential cryptanalysis usullarini takomillashtirishga bag‘ishlangan tadqiqotlarida neyron distinguisherlarni tayyorlash, kirish farqlarini tanlash va key-recovery bosqichlari samaradorligini oshirish masalalarini ko‘rib chiqdilar [4]. Keyingi tadqiqotlarda SIMON, SIMECK, SPECK kabi yengil blokli shifrlar uchun bir nechta shifrmatn juftliklaridan foydalanadigan distinguisherlar, ko‘p bosqichli neyron modellar hamda klassik differensial xususiyatlar bilan birlashtirilgan gibrid yondashuvlar rivojlantirildi. Bu ishlar sun’iy neyron tarmoqlar kriptotahlilda mustaqil vosita sifatida emas, ko‘pincha klassik kriptografik tahlil bilan integratsiyada samaraliroq bo‘lishini ko‘rsatadi.

AES bilan bog‘liq tadqiqotlarda ikki asosiy yo‘nalish kuzatiladi. Birinchi yo‘nalish qisqartirilgan raundli AESga nisbatan differential-neural distinguisherlarni qurish bilan bog‘liq. So‘nggi tadqiqotlarda Gohr arxitekturasi AESga moslashtirilib, ma’lum kirish farqiga ega ochiq matnlardan hosil qilingan shifrmatn juftliklarini tasodifiy juftliklardan ajratish imkoniyati tekshirilgan [12]. Ikkinchi yo‘nalish AESning amaliy implementatsiyalariga qarshi yon kanal tahlilidir. K. Kuroda, Y. Fukuda, K. Yoshida va hammualliflar maskalash himoyasi qo‘llangan AES dasturiy implementatsiyalarida chuqur o‘rganishga asoslangan yon kanal hujumlarining amaliy jihatlarini tadqiq qilganlar [3, 427–442-b.].

H. Wang va E. Dubrova FPGA muhitida amalga oshirilgan AESga qarshi tandem deep learning side-channel attack yondashuvini o‘rganib, neyron tarmoqlar apparat implementatsiyasidan olinadigan fizik sizib chiqishlarni tahlil qilishda ham qo‘llanishini ko‘rsatdilar [6]. Ushbu tadqiqotlar AESning matematik kriptobardoshliligi bilan uning konkret dasturiy yoki apparat implementatsiyasining xavfsizligi bir xil tushuncha emasligini ko‘rsatadi. Shu sababli neyron tarmoq

yordamida olingan natija qaysi xavf modeli va qaysi AES konfiguratsiyasiga tegishli ekanligi aniq ko‘rsatilishi kerak.

MDH mamlakatlari olimlari orasida ham sun’iy neyron tarmoqlar va axborot xavfsizligi kesishmasida tadqiqotlar olib borilmoqda. Rossiyalik S.S. Tarasenko 2023-yilda sun’iy neyron tarmoqlar va xatolarga bardoshli kodlashga asoslangan assimetrik kriptografik tizimning kriptobardoshliligini tadqiq qilib, neyron tarmoq komponentlaridan foydalanadigan kriptotizimlarni xavfsizlik nuqtayi nazaridan baholash masalasini ko‘rib chiqdi [10, 17–31-b.]. Bu ish MDH ilmiy makonida neyron tarmoqlarni faqat hujum vositasi emas, balki kriptografik tizim komponenti va tahlil obyekti sifatida ham o‘rganilayotganini ko‘rsatadi.

Rossiya ilmiy makonida neyron tarmoqlar kiberhujumlarni aniqlash va axborot xavfsizligi tizimlarini takomillashtirish uchun ham keng o‘rganilmoqda. T.M. Tatarnikova va I.A. Sikarev neyron tarmoqqa asoslangan hujumlarni aniqlash algoritmini ishlab chiqib, tarmoq arxitekturasini tanlash va o‘quv ma’lumotlarini normallashtirish masalalarini tajribaviy tahlil qilganlar [13]. Mazkur ish bevosita kriptotahlilga bag‘ishlanmagan bo‘lsa-da, neyron tarmoq arxitekturasini optimallashtirish, klassifikatsiya va xavfsizlikka oid ma’lumotlardan belgilarni ajratish kabi metodik jihatlari kriptografik ma’lumotlarni tahlil qilish tadqiqotlari uchun ham ahamiyatlidir.

O‘zbekistonda sun’iy neyron tarmoqlarni aynan kriptotahlilga tatbiq etishga bag‘ishlangan ochiq ilmiy adabiyotlar xorijiy tadqiqotlarga nisbatan hali cheklangan. So‘nggi yillarda Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti tadqiqotchilari Mirzo-Ulug‘bek Davlatov, Orif Allanov va Baxtiyor Turdibekov ushbu yo‘nalishda ish olib bordilar. Ularning 2025-yilda chop etilgan tadqiqotida Vigenère shifri misolida PyTorch asosidagi neyron tarmoq yordamida shifrmatndan statistik qonuniyatlarni o‘rganish va ochiq matnni qisman tiklash imkoniyatlari tekshirildi [11, 21–27-b.].

Davlatov, Allanov va Turdibekovning tadqiqoti O‘zbekistonda neyron tarmoqlarni klassik kriptotahlil jarayoniga qo‘llash bo‘yicha mahalliy tajribani shakllantirishga xizmat qiladi. Biroq klassik Vigenère shifridagi statistik bog‘lanishlar zamonaviy blokli shifrlardagi kuchli nolinearlik va diffuziya xususiyatlaridan sezilarli darajada farq qiladi. Shu sababli mahalliy tadqiqotlarni AES kabi zamonaviy blokli shifrlar, qisqartirilgan raundlar, kalit bitlarini klassifikatsiya qilish va giperparametrlarni avtomatik optimallashtirish yo‘nalishiga kengaytirish ilmiy jihatdan dolzarbdir.

Ko‘rib chiqilgan adabiyotlar shuni ko‘rsatadiki, xorijiy olimlar asosan neural distinguisher, differential-neural cryptanalysis, key-recovery va side-channel attack

yo‘nalishlarida sezilarli natijalarga erishgan. MDH tadqiqotlarida neyron tarmoqqa asoslangan kriptotizimlarning bardoshliligi va axborot xavfsizligi klassifikatsiyasi masalalari rivojlanmoqda. O‘zbekistonda esa neyron tarmoqlarning kriptotahlildagi qo‘llanilishi bo‘yicha dastlabki amaliy ishlar mavjud bo‘lsa-da, AES kalitlari yoki ularning bitlarini tasniflash, neyron tarmoq arxitekturasi va giperparametrlarini metaevristik usullar bilan birgalikda optimallashtirish masalalari yetarlicha yoritilmagan.

Mazkur ilmiy bo‘shliq ushbu tadqiqotning yo‘nalishini belgilaydi. Tadqiqotda soddalashtirilgan AES doirasida ochiq matn–shifrmatn juftliklaridan xususiyatlar shakllantirish, kalit bitlarini binar klassifikatsiya vazifasi sifatida ifodalash hamda sun’iy neyron tarmoqning arxitekturasi va asosiy giperparametrlarini optimallashtirish imkoniyatlari o‘rganiladi. Shu tariqa ish xorijiy neural cryptanalysis tajribasini mahalliy tadqiqotlar bilan bog‘lab, zamonaviy blokli shifrlar bo‘yicha eksperimental yondashuvni rivojlantirishga qaratiladi.

Sun’iy neyron tarmoq kriptotahlilda kirish ma’lumotlari X ni maqsadli natija Y ga moslashtiruvchi parametrik funksiya sifatida qaraladi: $\hat{Y}=f\theta(X)$. Kriptografik vazifada X ochiq matn, shifrmatn, ularning farqlari yoki ajratib olingan bitli belgilarni, Y esa distinguisher sinfi, kalit biti yoki oraliq qiymatni ifodalashi mumkin. Adabiyotlar tahlili modelning yuqori aniqligi o‘z-o‘zidan shifr buzilganini anglatmasligini ham ko‘rsatadi; natija raundlar soni, dataset tuzilishi, yangi kalitlarga umumlashtirish va tasodifiy bazaviy ko‘rsatkich bilan birgalikda baholanishi lozim.

Adabiyotlarda MLP, CNN va residual arxitekturalardan foydalanish uchraydi. Vektorli kriptografik belgilar uchun MLP qulay bo‘lsa, yon kanal trassalaridagi lokal naqshlarni aniqlashda CNN keng qo‘llanadi. Residual tarmoqlar esa chuqur arxitekturalarni barqaror o‘qitishga yordam beradi. Arxitektura, faollashtirish funksiyasi, learning rate, batch size va regulyarizatsiya parametrlarining maqbul kombinatsiyasi universal emas; shu sababli ularni validatsiya ma’lumotlari asosida optimallashtirish talab etiladi.

Umuman, so‘nggi ilmiy ishlar sun’iy neyron tarmoqlar kriptografik tahlilning istiqbolli yordamchi vositasi ekanini ko‘rsatmoqda. Shu bilan birga, ushbu yondashuvning ilmiy qiymati model natijalarining takrorlanuvchanligi, klassik kriptotahlil bilan qiyoslanishi, data leakage holatlarining oldini olish va tajriba chegaralarining aniq bayon qilinishiga bog‘liq. Mazkur talablar keyingi metodologik va eksperimental bosqichlarni shakllantirishda asos sifatida qabul qilindi.

1-jadval.

Sun’iy neyron tarmoqlarning kriptografiya va kriptotahlildagi asosiy qo‘llanish yo‘nalishlari.

Yo‘nalish	Kirish ma’lumoti	Maqsad	Asosiy cheklov
Neyron distinguisher	Shifrmatn juftliklari	Taqsimotlarni ajratish	To‘liq raundlarda signal juda zaif
Kalit bitlarini tasniflash	Ochiq matn–shifrmatn belgilar	Kalitga bog‘liq sinfni aniqlash	Data leakage va umumlashtirish
Differensial/linear + NN	Klassik kriptotahlil belgilari	Qaror bosqichini kuchaytirish	Natijani klassik baza bilan qiyoslash
Yon kanal tahlili	Quvvat/EM/vaqt trassalari	Oraliq qiymat yoki kalit bayti	Implementatsiyaga kuchli bog‘liqlik
Neyron kriptografiya	Xabar va kalit	O‘rganiladigan himoya sxemasi	Formal xavfsizlik kafolati cheklangan

TADQIQOT METODOLOGIYASI

Maqolada taklif etilayotgan metodik yondashuv besh bosqichdan iborat. Birinchi bosqichda kriptografik obyekt va hujum modeli belgilanadi: algoritm, raundlar soni, kalit uzunligi, hujumchiga ma’lum bo‘lgan ma’lumot va bashorat qilinadigan target aniq ko‘rsatiladi. Ikkinchi bosqichda dataset generatsiya qilinadi. Ochiq matnlar kriptografik xavfsiz tasodifiy generator yordamida olinadi, tegishli kalitlar bilan shifrlanadi va xususiyat vektorlari shakllantiriladi.

Uchinchi bosqichda ma’lumotlar trening, validatsiya va nazorat test to‘plamlariga ajratiladi. Eng muhim talab — test to‘plamining trening jarayonidan mustaqilligi. Agar maqsad yangi kalitlarga umumlashtirishni tekshirish bo‘lsa, kalit bo‘yicha ajratish amalga oshiriladi. Aks holda model bir xil kalitga xos naqshni yodlab olishi va sun’iy ravishda yuqori aniqlik ko‘rsatishi mumkin.

To‘rtinchi bosqichda neyron tarmoq arxitekturasi va giperparametrlari tanlanadi. Kirish o‘lchami d bo‘lgan MLP uchun h1,…,hk yashirin qatlamlar, faollashtirish funksiyasi, learning rate, batch size, epoch soni va regulyarizatsiya parametrlari belgilanadi. Binar kalit biti klassifikatsiyasida sigmoid chiqish va binary cross-entropy funksiyasi qo‘llanishi mumkin: $L=-[y\log(p)+(1-y)\log(1-p)]$.

Giperparametrlarni qo‘lda tanlash subyektivlikni oshiradi. Shu sababli genetik algoritm kabi metaevristik optimallashtirish usulidan foydalanish mumkin. Har bir individ tarmoq konfiguratsiyasini ifodalaydi; fitness funksiyasi validatsiya natijasiga asoslanadi. Selection, crossover va mutation operatorlari orqali yangi

avlod konfiguratsiyalari hosil qilinadi. Bunda nazorat test to‘plami giperparametr tanlash jarayoniga kiritilmasligi kerak.

Beshinchi bosqichda yakuniy model nazorat to‘plamida baholanadi. Accuracy bilan birga precision, recall, F1-score, ROC-AUC va confusion matrix keltirilishi maqsadga muvofiq. Sinflar muvozanatli binar vazifada 50 foizlik tasodifiy baza bilan statistik qiyoslash bajariladi. Bir nechta mustaqil ishga tushirishlar bo‘yicha o‘rtacha qiymat va standart og‘ish berilishi natijaning barqarorligini ko‘rsatadi.

Taklif etilayotgan modelda P ochiq matn, K maxfiy kalit va C=EK(P) shifrmatn sifatida olinadi. Xususiyatlar ajratish funksiyasi φ(P,C) orqali X∈{0,1}^32 ko‘rinishidagi 32 bitli vektor hosil qilinadi. Har bir j-kalit biti uchun yj=Kj∈{0,1} target belgilanadi. Neyron klassifikator fθj(X)→[0,1] tegishli bitning 1 bo‘lish ehtimolini baholaydi.

Modelni alohida bitlar bo‘yicha qurishning afzalligi shundaki, 2^n sinfli to‘liq kalit klassifikatsiyasi o‘rniga n ta binar vazifa hosil bo‘ladi. Bu o‘qitish jarayonini soddalashtiradi va qaysi bitlar tanlangan xususiyatlar orqali yaxshiroq ajralishini ko‘rsatadi. Kamchiligi esa bitlar orasidagi o‘zaro bog‘lanishlar to‘liq hisobga olinmasligidir. Keyingi tadqiqotlarda multi-task learning yoki umumiy feature extractor va bir nechta chiqish boshlaridan foydalanish mumkin.

Genetik algoritm yashirin qatlamlar soni, neyronlar soni, activation, learning rate, batch size va dropout koeffitsiyentini optimallashtirish uchun ishlatiladi. EarlyStopping va ModelCheckpoint esa genetik operator emas; ular o‘qitish jarayonini nazorat qiluvchi mexanizmlardir. EarlyStopping validatsiya ko‘rsatkichi yaxshilanmay qolganida ortiqcha o‘qitishni to‘xtatadi, ModelCheckpoint esa eng yaxshi parametrlar holatini saqlaydi.

Eksperimentning ilmiy qiymati faqat yuqori accuracy bilan emas, balki bazaviy modellar bilan adolatli qiyoslash orqali aniqlanadi. Logistic regression, SVM yoki oddiy MLP bazaviy model sifatida olinishi mumkin. Agar optimallashtirilgan neyron tarmoq ustun natija bersa, barcha modellar uchun dataset bo‘linishi, xususiyatlar va baholash mezonlari bir xil bo‘lishi zarur. Shundagina farq arxitektura va optimallashtirish ta’siri sifatida ehtiyotkorlik bilan talqin qilinadi.

2-jadval.

Neyron tarmoqqa asoslangan kriptotahlil eksperimentining tavsiya etiladigan ketma-ketligi.

Bosqich	Asosiy amal	Nazorat talabi
1. Muammo	Shifr va targetni aniqlash	Hujum modeli aniq

2. Dataset	P–C juftliklarini generatsiya qilish	Takror va leakage yo‘q
3. Bo‘lish	Train/validation/test	Test mustaqil
4. Optimallashtirish	NN + GA giperparametr tanlash	Test fitnessga kirmaydi
5. Baholash	Accuracy, F1, AUC	Bazaviy model bilan qiyos

TAHLIL VA NATIJALAR

Neyron kriptotahlilda natijani baholashning birinchi mezoni — modelning tasodifiy bazadan ishonchli yuqori natija ko‘rsatishidir. Biroq 50 foizdan biroz yuqori accuracy ham ayrim distinguisher vazifalarida kriptografik jihatdan qiziqarli bo‘lishi mumkin, chunki juda kichik statistik og‘ish ko‘p namunalar va key-recovery algoritmi bilan birlashtirilganda foydali signalga aylanishi ehtimoli mavjud. Shu sababli faqat umumiy accuracy emas, chiqish ehtimollari taqsimoti va kalit taxminlarini reytinglash qobiliyati ham o‘rganilishi kerak.

Ikkinchi mezon — umumlashtirish. Model faqat o‘qitishda uchragan kalitlar yoki ochiq matn shablonlarida yaxshi ishlasa, uning ilmiy xulosasi cheklangan bo‘ladi. Yangi kalitlar, boshqa random seedlar va mustaqil datasetda natijaning saqlanishi model haqiqatan ham umumiy kriptografik xususiyatni o‘rganganiga kuchliroq dalil beradi.

Uchinchi mezon — klassik kriptotahlil bilan qiyoslash. Neural differential cryptanalysis bo‘yicha keyingi ishlar Gohr yondashuvini rivojlantirib, neyron distinguisherlarning qaysi xususiyatlarni o‘rganishi va ularning klassik differensial xususiyatlarga nisbatan afzalligi qayerdan kelishini tushuntirishga harakat qilmoqda [7]. Bu tendensiya “qora quti” aniqligidan tashqari interpretatsiyaga e’tibor kuchayayotganini ko‘rsatadi.

To‘rtinchi mezon — hisoblash murakkabligi. Neyron modelni o‘qitish uchun katta dataset va GPU resurslari talab qilinishi mumkin. Shuning uchun modelning inference tezligi, o‘qitish vaqti, xotira sarfi va ma’lumotlar murakkabligi ham klassik usullar bilan bir qatorda keltirilishi kerak. Kriptotahlilda faqat accuracy emas, hujumning vaqt, ma’lumot va xotira murakkabligi asosiy mezonlardan hisoblanadi.

Beshinchi mezon — natijaning xavfsizlik doirasini to‘g‘ri ifodalash. Qisqartirilgan raundli shifrda yoki yon kanalga ega implementatsiyada olingan natija to‘liq standart AESning matematik xavfsizligi buzilganini bildirmaydi. Zamonaviy sharhlarda to‘liq AESga qarshi ma’lum klassik va gibrid hujumlarning amaliy

cheklovlari qayd etiladi [8]. Ilmiy maqolada ushbu chegarani aniq ko‘rsatish natijaning ishonchliligini oshiradi.

SUN’IY NEYRON TARMOQLARNING AFZALLIKLARI VA CHEKLOVLARI

Sun’iy neyron tarmoqlarning asosiy afzalligi murakkab nolinear bog‘lanishlarni oldindan qat’iy analitik model bermasdan o‘rganishidir. Bu xususiyat katta hajmdagi kriptografik kuzatuvlar, ayniqsa yon kanal trassalari bilan ishlashda muhim. Bundan tashqari, feature learning imkoniyati qo‘lda belgi ajratishga bo‘lgan ehtiyojni kamaytirishi mumkin.

Shu bilan birga, kriptografik ma’lumot ataylab statistik tuzilmani yashirish uchun yaratiladi. Shuning uchun oddiy ma’lumotlar to‘plamlarida muvaffaqiyatli bo‘lgan neyron arxitektura kuchli shifrda foydali signal topa olmasligi tabiiy. Modelning muvaffaqiyatsizligi ham ilmiy natija bo‘lishi mumkin: u tanlangan xususiyatlar va hujum modeli doirasida ajratuvchi signal aniqlanmaganini ko‘rsatadi.

Interpretatsiya muammosi yana bir cheklovdir. Neyron tarmoq nima sababdan ma’lum sinfni tanlaganini tushuntirish klassik differensial xarakteristika yoki chiziqli approksimatsiyaga qaraganda qiyinroq. Gradient tahlili, feature attribution, ablation va kirish bitlarini maskalash kabi usullar qaysi komponentlar model qaroriga ko‘proq ta’sir qilganini tekshirishga yordam beradi.

Reproduktivlik ham muhim. Dataset generatsiya kodi, kalit va plaintext generatsiyasi qoidalari, random seed, arxitektura, optimizer, learning rate, batch size, epoch, early stopping sharti va apparat muhiti batafsil ko‘rsatilishi lozim. Aks holda yuqori natijani mustaqil takrorlash qiyinlashadi.

XULOSA VA TAKLIFLAR

Sun’iy neyron tarmoqlar kriptografiya va kriptotahlilning an’anaviy matematik usullarini almashtiruvchi universal vosita emas, balki ma’lum sharoitlarda ularni to‘ldiruvchi kuchli hisoblash yondashuvidir. Neyron distinguisherlar, kalitga bog‘liq klassifikatsiya, gibrid differensial va chiziqli tahlil hamda yon kanal hujumlari ushbu yo‘nalishning eng muhim amaliy ko‘rinishlaridir.

AES misolida neyron tarmoqlarni qo‘llashda to‘liq standart shifrning matematik xavfsizligi, qisqartirilgan yoki soddalashtirilgan model va implementatsion yon kanal zaifliklarini bir-biridan qat’iy ajratish zarur. Ilmiy jihatdan ishonchli natija uchun mustaqil test to‘plami, bazaviy modellar, takroriy eksperimentlar va hisoblash murakkabligi bahosi talab etiladi.

Kelgusida giperparametrlarni genetik algoritm yordamida optimallashtirish, bitlar bo‘yicha klassifikatsiyani multi-task arxitektura bilan birlashtirish,

interpretatsiya usullarini qo‘llash va modelning yangi kalitlarga umumlashtirish qobiliyatini tekshirish istiqbolli yo‘nalishlar hisoblanadi. Bunday yondashuv sun’iy neyron tarmoqlarning kriptotahlildagi real imkoniyatlarini ortiqcha da’volarsiz, tajribaviy va takrorlanuvchi tarzda baholash imkonini beradi.

Kriptografiyada neyron tarmoqdan foydalanadigan tadqiqotlarda birinchi navbatda aniq xavf modeli yozilishi tavsiya etiladi. “AES kalitini neyron tarmoq bilan topish” kabi umumiy ifoda o‘rniga qaysi raundlar, qanday ma’lumot, qanday kalit taqsimoti va qaysi target o‘rganilayotgani ko‘rsatilishi kerak.

Ikkinchidan, ma’lumotlar bazasini shakllantirishda trening va test o‘rtasida kalit, plaintext yoki generatsiya seedlari orqali yashirin bog‘lanish paydo bo‘lmasligi nazorat qilinishi zarur. Uchinchi tomondan, har bir tajriba oddiy bazaviy model va tasodifiy klassifikator bilan qiyoslanishi kerak.

To‘rtinchidan, giperparametr optimallashtirish natijasini baholashda validatsiya va yakuniy test vazifalari ajratilishi kerak. Genetik algoritm fitnessni validatsiyada optimallashtiradi; test esa faqat yakuniy tanlangan modelga bir marta xolis baho berish uchun ishlatiladi.

Beshinchidan, AES kabi standart algoritmlar bilan bog‘liq xulosalarda “algoritm buzildi” degan keng da’volardan qochib, aynan tajriba doirasi ko‘rsatilishi lozim. Bu ilmiy aniqlikni saqlaydi va neyron kriptotahlilning haqiqiy hissasini aniqroq ko‘rsatadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. **Daemen J., Rijmen V.** The Design of Rijndael: The Advanced Encryption Standard (AES). — 2nd ed. — Berlin; Heidelberg: Springer, 2020. — 282 p. (Springer Nature)

2. **Gohr A.** Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning // Advances in Cryptology – CRYPTO 2019. — Springer, 2019. — P. 150–179.

3. **Kuroda K., Fukuda Y., Yoshida K. et al.** Practical Aspects on Non-Profiled Deep-Learning Side-Channel Attacks Against AES Software Implementation with Two Types of Masking Countermeasures Including RSM // Journal of Cryptographic Engineering. — 2023. — Vol. 13. — P. 427–442.

4. **Lu J. et al.** Improving Differential-Neural Cryptanalysis. — Cryptology ePrint Archive, Report 2022/183, 2022.

5. **Improved Machine Learning-Aided Linear Cryptanalysis: Application to DES** // Cybersecurity. — 2024.

6. **Wang H., Dubrova E.** Tandem Deep Learning Side-Channel Attack on FPGA Implementation of AES // SN Computer Science. — 2021. — Vol. 2. — Article 373.

7. **SoK: 5 Years of Neural Differential Cryptanalysis.** — Cryptology ePrint Archive, Report 2024/1300, 2024.

8. **A Panoramic Survey of the Advanced Encryption Standard: From Architecture to Security Analysis, Key Management, Real-World Applications, and Post-Quantum Challenges** // International Journal of Information Security. — 2025.

9. **Benamira A., Gérault D., Peyrin T., Tan Q. Q.** A Deeper Look at Machine Learning-Based Cryptanalysis // Advances in Cryptology – EUROCRYPT 2021. — Springer, 2021.

10. **Tarasenko S. S.** Issledovanie kriptostoykosti asimmetrichnoy kriptograficheskoy sistemy, osnovannoy na iskusstvennykh neyronnykh setyakh s primeneniem pomekhoustoychivogo kodirovaniya // Telekommunikatsii. — 2023. — № 3. — S. 17–31.

11. **Davlatov M.-U., Allanov O., Turdibekov B.** Application of Neural Networks in Cryptanalysis: The Case of the Vigenère Algorithm // American Journal of Applied Science and Technology. — 2025. — Vol. 5, Issue 12. — P. 21–27. DOI: 10.37547/ajast/Volume05Issue12-04.

12. **Differential-Neural Cryptanalysis on AES** // IEICE Transactions on Information and Systems. — 2024. DOI: 10.1587/transinf.2024EDL8044.

13. **Tatarnikova T. M., Sikarev I. A.** Obnaruzhenie atak metodom iskusstvennykh neyronnykh setey // Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy. — 2023. — № 4. — S. 84–94.