Deep learning usullari va ularning kriptotahlil masalalarida qo‘llanilishi

Rahmatullayev Ilhom Raxmatullayevich,
Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti doktoranti
Toshkent Kimyo xalqaro universiteti Samarqand filiali
ilhom9001@gmail.com

Abduraximov Baxtiyor Fayziyevich,
Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti,
a_baxtiyor@mail.ru

Annotatsiya. Ushbu maqolada chuqur o‘rganish (deep learning) texnikalarining zamonaviy kriptotahlil jarayonlarida qo‘llanilish imkoniyatlari nazariy va eksperimental jihatdan tahlil qilingan. An’anaviy kriptoanaliz usullari kalit, ochiq matn va shifr matni o‘rtasidagi murakkab chiziqsiz bog‘lanishlarni aniqlashni talab qilgani sababli yuqori hisoblash murakkabligiga ega. Deep learning esa xom ma’lumotlar bilan bevosita ishlash, xususiyatlarni mustaqil ravishda ajrata olish va biaslarni avtomatik aniqlash kabi ustunliklari sababli kriptotizimlarning zaifliklarini topishda samarali vosita sifatida namoyon bo‘lmoqda. Tadqiqotda oqimli shifrlar — RC4, uning takomillashtirilgan varianti RC4A, shuningdek Trivium va TRIAD algoritmlarining hosil qilgan keystreamlari "qora quti" modeli asosida chuqur neyron tarmoqlar orqali tahlil qilindi.

Kalit so‘zlar: Deep Learning, Chuqur O‘rganish, Neyron Tarmoqlar, Kriptotahlil, Oqimli Shifrlash, RC4, RC4A, Trivium, TRIAD, Black-Box Modeli, Keystream, Bias Aniqlash, Mashinali O‘qitish, Konvolyutsion Neyron Tarmoqlar (CNN), Rekurrent Neyron Tarmoqlar (RNN), LSTM, Differensial Kriptoanaliz, Yon Kanal Tahlili, Kriptografiya.

I. Kirish.

An’anaviy kriptoanaliz usullari oddiy ma'lumot (plaintext), kalit va tegishli shifr matni (ciphertext) orasidagi bog‘lanishni belgilovchi chiziqsiz akslantirishlarni keng qamrovda tahlil qilishni talab qiladi. Bu akslantirishlarni ifodalovchi funksiyalarning darajasi juda yuqori bo‘ladi va kriptoanaliz ishini juda qiyinlashtiradi. Deep learning algoritmlari va samarali hisoblash resurslarining paydo bo‘lishi shifr ma'lumotini qayta ishlanmagan ko‘rinishda (raw form) tahlil qilish uchun yangi imkoniyatlar yaratdi.

Shifrlashning asosiy tamoyili - tizimga tasodifiylik kiritish, ya'ni shifr ma'lumotida hech qanday bog’liklik bo‘lmasligi kerak. Shu sababdan shifr ma'lumotini qayta ishlanmagan ko‘rinishda tahlil qilish zarur. Deep learning algoritmlari an'anaviy mashina o‘qitishdan farq qiladi: ular qayta ishlanmagan ma'lumot bilan bevosita ishlaydi va alohida xususiyat (feature) tanlash yoki ajratish talab qilinmaydi.

Ushbu g‘oya va deep learning algoritmlarining shifr ma'lumotiga mos kelishi taxmini asosida oqimli shifrlarda (stream ciphers) **black-box** (qora quti) tahlil modelida bias (tasodifiylikdan chetlanish) topish uchun deep learning usulini qo‘llash mumkin. Taklif qilingan usul maqsadi - oqimli shifr tomonidan yaratilgan keystream-ning aniq joyidagi chiqish bit/byte (output bit/byte) sodir bo‘lish ehtimolini bashorat qilishdir. Quyida ushbu yondashuvning RC4 va uning yaxshilangan varianti RC4A ustida sinab ko‘rishdan olingan natijalar batafsil muhokama qilinadi.

Shuningdek, taklif qilingan usul Trivium va TRIAD oqimli shifrlari ustida ham qo‘llab ko‘rilgan. Taklif qilingan yondashuv RC4 dagi og‘ishni (bias) aniqlay oladi, ammo uning yaxshilangan varianti (RC4A) hamda Trivium va TRIAD’da bunday og‘ish mavjud emasligini ko‘rsatadi. RC4 ga e'tibor qaratgan holda yondashuvni mavjud usullarga nisbatan yondashuv jihatidan va kuzatuvlar nuqtai nazaridan

solishtirib, taklif qilingan usul soddaroq va ekanligini ko‘rish mumkin.

II. Metodologiya

Deep Learning - bu zamonaviy mashinali o‘qitish usullarining yangi va tez rivojlanayotgan yo‘nalishi bo‘lib, uning asosini sun’iy neyron tarmoqlar (Artificial Neural Networks) tashkil etadi. Deep learning, ya’ni chuqur o‘rganish tizimlari, Recurrent Neural Network (RNN), Deep Belief Network (DBN) hamda Convolutional Neural Network (CNN) kabi turli arxitekturalarga ega bo‘lib, ular tabiiy tilni qayta ishlash, mashina tarjimasi, tibbiy tasvirlarni qayta ishlash, kompyuter ko‘rish tizimlari va boshqa murakkab masalalarni hal qilishda keng qo‘llanadi [1,2]. Ushbu arxitekturalar ko‘plab sohalarda yuqori natijalar ko‘rsatib, ba’zi hollarda inson mutaxassislarining ko‘rsatkichlaridan ham ustun bo‘lgan. Deep learning’ning an’anaviy mashinali o‘qitish algoritmlariga nisbatan asosiy ustunliklaridan biri - bu tasvirlash (representation learning) imkoniyatidir. Representation learning - xom ma’lumotlardan belgi (feature) aniqlash uchun zarur bo‘lgan tasvirlarni avtomatik yaratishga qaratilgan metodlar sinfidir. Mazkur yondashuv mashinali o‘qitish vazifalari (tasniflash, regressiya va boshqalar) uchun kirish ma’lumotlarini kompyuter tomonidan samarali qayta ishlanishi mumkin bo‘lgan shaklga keltirishda muhim ahamiyatga ega. Umuman olganda, deep learning - bir nechta yashirin qatlamlarga ega sun’iy neyron tarmoqlar yordamida xom kirish ma’lumotlaridan mazmunli xususiyatlarni o‘rganishga mo‘ljallangan algoritmlar majmuasidir.

Kriptotahlil bo‘yicha ko‘plab mustahkam va yaxshi ishlab chiqilgan usullar mavjud. Biroq bu usullarning amaliy qo‘llanishida eng muhim bosqich - shifrlash algoritmidagi ichki zaiflikni topish va undan foydalanib hujumni amalga oshirishdir. Bu jarayon juda murakkab bo‘lib, ko‘pincha yuqori darajadagi matematik bilimlar va katta hisoblash resurslarini talab qiladi. Shu nuqtai nazardan deep learning metodlarining xom ma’lumotlardan avtomatik tarzda xususiyat ajratish imkoniyati kriptotahlilni eng muhimi - zaiflikni aniqlash bosqichida sezilarli darajada yengillashtirishi mumkin.

Oqimli shifrlar uchun generatsiya qilinadigan gamma ketma-ketligi (keystream) mutlaqo og‘ishlarsiz bo‘lishi shart. Agar unda statistik og‘ishlar yoki korrelyatsiyalar mavjud bo‘lsa, tahlilchi ushbu og‘ishlardan foydalanib kalit yoki ochiq ma’lumot haqida qisman yoki to‘liq bilimga ega bo‘lishi mumkin. Shu bois, murakkab kriptotahliliy usullarni qo‘llashdan avval deep learning asosidagi avtomatik tahlil yordamida bunday og‘ishlarni aniqlab olish alohida ahamiyatga ega.

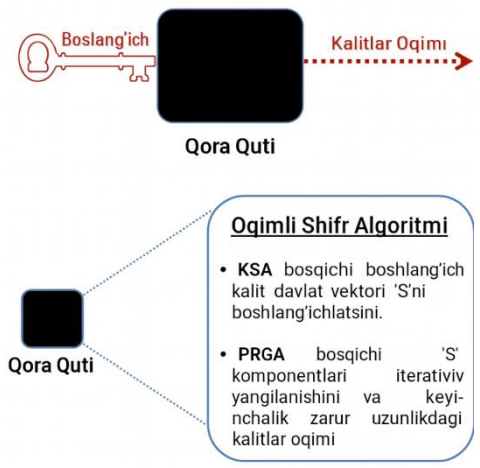
Mashinali o‘qitish, ayniqsa deep learning’ning kriptografiyaga qo‘llanilishi ilmiy adabiyotlarda uzoq vaqt davomida juda chegaralangan tarzda o‘rganib kelingan. Rivestning mashhur tadqiqotlaridan birida mashinali o‘qitish va kriptotahlil “opa-singil sohalar” sifatida tasvirlanadi, chunki ikkisi ham kirish–chiqish juftliklariga asoslangan noma’lum funksiyani o‘rganishni maqsad qiladi [4].

So‘nggi yillarda ushbu yo‘nalish bo‘yicha sezilarli yutuqlar kuzatilmoqda. Masalan, Abadi va Andersen neyron tarmoqlar ko‘p agentli tizimda boshqa neyron tarmoqlardan axborotni himoya qilish uchun maxfiy kalitlardan foydalanishni o‘rganishi mumkinligini amaliy jihatdan ko‘rsatdi [5]. Hesamifard va hammualliflar shifrlangan ma’lumotlar ustida chuqur neyron tarmoqlarni ishga tushirish uchun yangi maxfiylikni ta’minlovchi metodlarni ishlab chiqdi [6]. Picek va hamkorlar konvolyutsion neyron tarmoqlarning yon kanal tahlili (side-channel analysis) uchun samaradorligini tajribaviy tekshirib, deep learning boshqa mashinali o‘qitish usullariga qaraganda bu sohada ko‘proq ustunlikka ega bo‘lishi mumkinligi haqidagi muhim savolni ilgari surdi [7]. Wang AES blok shifriga nisbatan chuqur o‘rganish asosidagi yon kanal tahlilini amalga oshirdi [8]. Yengil blokli shifrlashning rivojlanishida Gohr tomonidan taklif etilgan yondashuv alohida ajralib turadi [9]. U Speck32/64 shifrining qisqartirilgan raundlariga nisbatan chuqur o‘rganish bilan kuchaytirilgan yaxshilangan kriptotahliliy hujumlarni taklif qildi [10]. Bu [9] ish neyron tarmoqlarni klassik kriptotahlil usullari bilan birlashtirishning birinchi y katta maqsadli namunasi bo‘lib, mavjud natijalardan yaxshiroq samaradorlikka erishdi. Ushbu yo‘nalish keyinchalik

Baksi va boshqalar, Jain va boshqalar [2] hamda Yadav va boshqalar [3] tomonidan davom ettirilgan va differensial kriptotahlilning mashinali o‘qitish bilan birlashtirilganda sezilarli darajada samarali bo‘lishi isbotlangan. Yaqinda Xiao va hammualliflar shifr kuchini neyron tarmog‘ining ushbu shifrlagichni taqlid qila olish qiyinligi orqali miqdoriy baholash metodini ishlab chiqdi. Ular shifrlagich moslik darajasi, o‘qitish ma’lumotlari murakkabligi, o‘qitish vaqti murakkabligi kabi yangi metrikalarni taklif qildi. Tadqiqot natijalari mashhur avtomobil xavfsizligida qo‘llaniladigan Hitag2 oqimli shifri hatto uch raundli DES shifridan ham zaifroq ekanligini ko‘rsatdi. Mavjud adabiyotlar tahlili shuni ko‘rsatadiki, so‘nggi yillarda kriptografiya bo‘yicha ilmiy jamoa deep learning’ni kriptografiyaga tatbiq etish bo‘yicha faol va chuqur tadqiqotlar olib bormoqda. Ushbu yo‘nalish kelajakda yanada kengayishi va zamonaviy kriptotahlilning eng muhim tarkibiy qismi bo‘lishi kutilmoqda.

III.Asosiy qism

Ushbu ishda chuqur o‘rganishga asoslangan yondashuv taklif etiladi. Taklif etilgan metod deep learning texnikalarining afzalliklariga mos keladi, chunki bu texnikalarda xususiyatlarni ajratish yoki xususiyatlarni tanlash (feature extraction/feature selection) jarayonlari talab etilmaydi. Aks holda, bunday bosqichlar har qanday matematik, statistik yoki analitik usullarda chetlab o‘tilmaydi. Chuqur o‘rganish esa zarur bo‘lgan xususiyatlarni xom ma’lumotlardan bosqichma-bosqich o‘zi o‘rganib boradi. Taklif etilgan yondashuv masalani “qora quti” (black-box) ssenariysi sifatida ko‘rib chiqadi (1-rasm).



1-rasm. Taklif qilingan usul uchun “Qora quti” tahlil modeli

“Qora quti” qurilmasi uning ichki mexanizmlaridan xabarsiz holda faqat kirish va chiqishlari orqali tavsiflanadigan tizim sifatida talqin qilinadi. Bizning tajribalarimizda oqimli shifr algoritmi qora quti sifatida qabul qilinadi va masala klassifikatsiya vazifasi ko‘rinishida qo‘yiladi. Maqsad - berilgan kirishdan foydalanib, chiqishning ma’lum bir pozitsiyasidagi qiymatni bashorat qilishdir. Taklif etilgan yondashuvning tajriba natijalaridan olingan xulosalar quyidagilardan iborat:

– tadqiqot natijalari shuni ko‘rsatadiki, oqimli shifrlarni tahlil qilish uchun chuqur o‘rganishga asoslangan yondashuv mavjud usullarga nisbatan ancha sodda va afzalliklarga ega.
– taklif etilgan metodning RC4 oqimli shifri va uning yaxshilangan turi — RC4A bo‘yicha keng qamrovli tahlil orqali tasdiqlanishi chuqur o‘rganish yondashuvlarining shifrlash ma’lumotlarini qayta ishlashda qo‘llanishini amalda isbotlaydi.
– olingan samaradorlik natijalari ushbu yondashuvning boshqa oqimli shifrlarga umumlashtirilishi mumkinligini ko‘rsatadi.

Chuqur o‘rganish usullari (Deep Learning Methods)

Chuqur o‘rganish - bu sun’iy neyron tarmoqlarining bir nechta qatlamlarini ketma-ket qo‘llab, xom kirish ma’lumotlaridan yuqori darajadagi xususiyatlarni ajratib olishga mo‘ljallangan mashinani o‘rganish algoritmlari sinfi hisoblanadi [4]. Masalan, tasvirlarni qayta ishlashda dastlabki pastki qatlamlar chetlarni aniqlasa, yuqori qatlamlar raqamlar, harflar yoki yuzlar kabi mazmunli xususiyatlarni ajratadi. 2-rasmda kirish va chiqish qatlamlari hamda bir nechta oraliq yashirin qatlamlardan iborat umumiy chuqur o‘rganish (deep learning) arxitekturasi ko‘rsatilgan.

Neyron tarmoqlarda gradientning yo‘qolishi muammosi [5] va hisoblash cheklovlari sababli bir necha yil oldin ko‘p qatlamli neyron tarmoqlarini o‘qitish imkonsiz yoki hisoblash jihatdan qiyin bo‘lgan. Biroq so‘nggi o‘n yillikda GPU (Graphical Processing Unit) va Google tomonidan TPU (Tensor

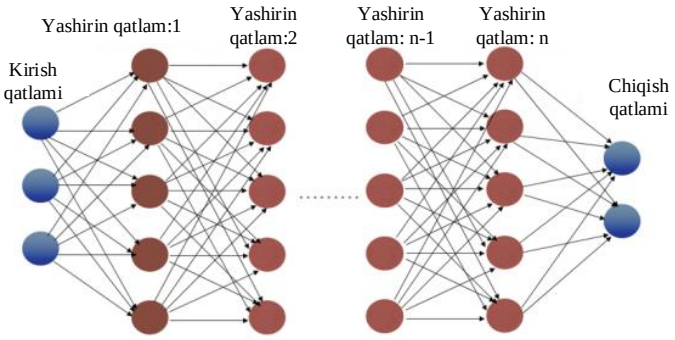
Processing Unit) kabi kuchli hisoblash vositalarining rivojlanishi hamda klassik sigmoid funksiyasi o‘rniga ReLU (Rectified Linear Unit) faollashtirish funksiyasining joriy etilishi tufayli neyron tarmoqning bir nechta yashirin qatlamlarini qo‘llash mumkin bo‘ldi [6]. ReLU va Sigmoid faollashtirish funksiyalari mos ravishda quyidagicha aniqlanadi:

$$f(x) = max(0, x), g(x) = \frac{1}{1+e^{-x}}.$$

Kirish qatlamida xom ma’lumot qabul qilinadi, oraliq yashirin qatlamlar esa faollashtirish funksiyasidan foydalanib ma’lumotlarni bosqichma-bosqich qayta ishlaydi. Chiqish qatlamida esa odatda yakuniy tasniflash uchun Softmax funksiyasi qo‘llanadi. Softmax funksiyasi quyidagicha ifodalanadi:

$$F(X)_i = \frac{e^{x_i}}{\sum_k e^{x_k}}, i = 0,1,2, \dots, k$$

bu yerda k mumkin bo‘lgan chiqishlar sonini bildiradi. Kirish va chiqish qatlamlari orasiga ko‘p yashirin qatlamlarni qo‘yish tarmoqlarga kirish ma’lumotlarini mos keluvchi chiqish ma’lumotlariga abstrakt tarzda xaritalashni o‘rganishga imkon beradi.



2-rasm. Umumiy chuqur o‘rganishning (Deep Learning) arxitekturasi

Eng mashhur chuqur o‘rganish texnikalaridan ba’zilari quyidagilar: Konvolyutsion Neyron Tarmoqlari (CNN), Rekurrent Neyron Tarmoqlari (RNN) va Uzun-Qisqa Muddatli Xotira tarmoqlari (LSTM) [7].

Oqimli shifrlash algoritmlarining qisqacha tavsifi

Simmetrik kalitli kriptografiya blokli shifrlash va oqimli shifrlash algoritmlaridan iborat. Oqimli shifrlashda boshlang‘ich kalit (odatda maxfiy kalit deb yuritiladi) asosida kerakli uzunlikdagi kalit oqimi (keystream) hosil qilinadi. Ushbu kalit oqimi so‘ngra (odatda XOR amali orqali) ochiq matn bitlari bilan birlashtirilib, shifrlangan matn (ciphertext) hosil qilinadi.

Zamonaviy kriptografiyaning dastlabki davrlarida oqimli shifrlash algoritmlari blokli shifrlashga nisbatan soddaligi va yuqori tezligi tufayli keng qo‘llanilgan. Oqimli shifrlash yuqori o‘tkazuvchanlik talab qilinadigan yoki past murakkablikdagi apparat resurslari mavjud bo‘lgan tizimlarda afzal variant bo‘lib kelgan.

Kriptografiyaning asosiy talablari nuqtai nazaridan, oqimli shifrlash algoritmi chiqishdagi kalit oqimining tasodifiylik xususiyatlarini ta’minlashi lozim. Buni amalga oshirish mezonlaridan biri — oqimli shifrlagich tomonidan hosil qilingan har bir bayt pozitsiyasida 0 dan 255 gacha bo‘lgan har qanday qiymatning paydo bo‘lish ehtimoli teng bo‘lishidir. Ya’ni har bir qiymatning paydo bo‘lish ehtimoli 1/256 bo‘lishi kerak. Agar ma’lum bir bayt pozitsiyasida qiymatlarning paydo bo‘lish ehtimoli bundan sezilarli darajada farq qilsa, kalit oqimida og‘ish (bias) mavjud deb hisoblanadi.

Bunday statistik og‘ish oqimli shifrlagichni kriptotahlilga nisbatan zaiflashtiradi.

IV. Natijalar

RC4 oqimli shifrlash algoritmi keystreamni baytma-bayt iterativ tarzda hosil qiladi. Yaratuvchilari RC4 tomonidan hosil qilinadigan oqim psevdotasodifiy xususiyatlarga ega ekanini ta’kidlagan. Shifrlash jarayonida ochiq matn baytlari keystream baytlari bilan XOR qilinadi. Xuddi shu amal teskari yo‘nalishda bajarilib, shifrdan ochish (decryption) amalga oshiriladi — ciphertext baytlari keystream baytlari bilan bitma-bit XOR qilinadi.

RC4 algoritmi ikki asosiy bosqichdan iborat:

- KSA (Key Scheduling Algorithm) — boshlang‘ich holatni (state) kalit asosida aralashtiradi.
- PRGA (Pseudo Random Generation Algorithm) — psevdotasodifiy baytlar oqimini generatsiya qiladi.

Algoritmning rasmiy tavsifi 1-algoritmda keltirilgan, RC4 oqimli shifrlagichining soddalashtirilgan tuzilmasi esa 2-rasmda ko‘rsatilgan.

RC4 oqimli shifrlash algoritmi bo‘lib, u SSL(Secure Sockets Layer) protokoli va WEP (simsiz tarmoqlarda xavfsizlikni ta’minlashda) keng foydalaniladi. RC4 oqimli shifrlash algoritmi Ron Rivest tomonidan 1987-yilda yaratilgan va shuning uchun RC4(Rivest Cipher 4) deb nomlangan.

RC4 psevdotasodifiy bitlar ketma-ketligini hosil qiladi va quyidagi ikki qismdan iborat bo‘lgan maxfiy oraliq holatidan foydalaniladi:

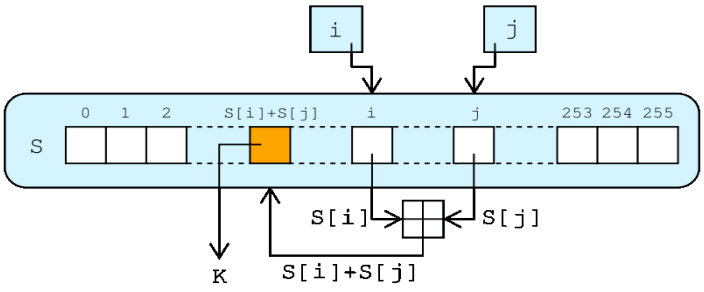
- barcha mumkin bo‘lgan 256 baytning joylashishdagi o‘rni(*S* ni topish);
- ikkita 8 – bitli indekslar (*i* va *j* larni topish).

Baytlarning kelish tartibi kalit uzunligi bilan amalga oshiriladi, odatda 40-256 bit oralig‘ida bo‘lib, kalit jadvali(key-scheduling) algoritmi orqali hosil qilinadi. Bu jarayon tugagandan so‘ng psevdotasodifiy sonlar generatori algoritmi yordamida bitlar ketma-ketligi hosil qilinadi.

Kalit jadvali algoritmi quyidagicha:

for i from 0 to 255
S[i]:=i
endfor
j:=0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
swap values of S[i] and S[j]
endfor

Psevdotasodifiy sonlar generatori algoritmi orqali hosil bo‘lgan ketma-ketlik tanlangan $S(i)$ va $S(j)$ o‘zgaruvchilarni *mod256* bo‘yicha qo‘shishdan hosil bo‘ladi (3-rasm).



3-rasm. RC4 generatori almashtirishi

Psevdotasodifiy sonlar generatori algoritmi quyidagicha:

i := 0
j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap values of S[i] and S[j]
k := inputByte XOR S[(S[i] + S[j]) mod 256]
output K
endwhile

Algoritmda *i* o‘zgaruvchini qiymati ortishi bilan hosil bo‘lgan baytlar soni ham ortib boradi.

Bu yerda almashtirish funksiyasi *swap* quyidagi ko‘rinishga ega:

byte temp = array[ind1];
array[ind1] = array[ind2];
array[ind2] = temp;

Ushbu generator kriptobardoshli sanalib, xususiyati kiruvchi kalit tasodifiylik darajasi bilan belgilanadi. Hozirda ushbu algoritmning bir nechta variantlari mavjud bo‘lib (RC4A, VMPC, RC4+), ularda dastlabkilarida mavjud kamchiliklar bartaraf etilgan.

Algoritmik jarayonda RC4 tomonidan qo‘llaniladigan “+” belgi N modul bo‘yicha qo‘shish amalini bildiradi. KSA (Key Scheduling Algorithm) bosqichida massiv *S[]* ning N ta juft elementi maxfiy kalit (*key*) qiymatlariga asoslanib o‘zaro almashtiriladi. KSA bosqichi yakunida PRGA uchun boshlang‘ich holat shakllantiriladi. Shundan so‘ng, algoritmning PRGA bosqichida kerakli uzunlikdagi kalit oqimi (keystream) generatsiya qilinadi.

Paul va Praneel[19] RC4 oqimli shifrlash algoritmida zaiflik mavjudligini aniqlaganlar, va ushbu muammoni bartaraf etish maqsadida yaxshilangan varianti - RC4A algoritmini taklif qilganlar. RC4A oqimli shifrlagichi bitta massiv o‘rniga ikki alohida holat massivini - S_1 va S_2 ni hosil qilish uchun RC4 ning KSA bosqichiga tayanadi. RC4A ning psevdotasodifiy oqim generatsiyasi (PRGA) algoritmidagi qolgan bosqichlar RC4 dagi kabi deyarli bir xil tarzda bajariladi.

Yuqorida qayd etilganidek, taklif etilgan usul yana ikki oqimli shifrlash algoritmlari – Trivium [8] va TRIAD [9] -- ustida ham sinovdan o‘tkaziladi. Trivium

oqimli shifrlash algoritmi dizayn jihatidan maksimal darajada soddalashtirilgan bo‘lishi, shu bilan birga zarur xavfsizlik darajasi, tezlik va moslashuvchanlik ta’minlanishi uchun yaratilgan. Trivium uzoq yillar davomida chuqur kriptotahlildan o‘tgan va hozirga qadar unga qarshi brute-force’dan kuchliroq hujumlar aniqlanmagan. Shu sababli, ushbu shifrlash algoritmida ham kalit oqimidagi biaslarni aniqlash mumkinligi tekshiriladi.

Boshqa tomondan, TRIAD-SC nisbatan yangi bo‘lib, uning asosida NIST Lightweight Cipher tanlovida taqdim etilgan yengil vaznli simmetrik shifrlash algoritmlari oilasi yaratilgan. TRIAD-SC bo‘yicha samarali kriptotahlil ishlari hali mavjud emas, shuning uchun ushbu oqimli shifrlash algoritmi tomonidan generatsiya qilingan keystreamdagi ehtimoliy og‘ishlarni aniqlash imkoniyati ham o‘rganiladi.

Trivium sinxron oqimli shifr bo‘lib, asosan apparat (hardware) muhitida samarali ishlash uchun loyihalangan, biroq dasturiy (software) muhitda ham yetarlicha yuqori unumdorlikka ega. Trivium dizaynerlari tomonidan eSTREAM tanloviga [10] taqdim etilgan va keyinchalik bu loyihaning 2-profili uchun tavsiya etilgan. 2-profil kichik maydonli apparat shifrlari uchun mo‘ljallangan. Trivium 80-bitli kalit va 80-bitli IV asosida 2^{64} bitgacha chiqish oqimini generatsiya qiladi. Boshqa texnik tafsilotlar ular [20] ishda batafsil yoritilgan.

TRIAD - oqimli shifrlash asosidagi kriptografik oiladir va u ikkita asosiy komponentdan iborat: autentifikatsiyalovchi shifrlash rejimi (TRIAD-AE) va xesh funksiyasi (TRIAD-HASH). TRIAD-AE “shifrlash + MAC” konstruksiyasiga asoslangan bo‘lib, bu yerda TRIAD-SC oqimli shifr shifrlash modulini bajaradi. TRIAD oilasi NIST ning yengil vaznli kriptografiya standarti tanloviga taqdim etilgan [11].

TRIAD-SC algoritmi 128-bitli maxfiy kalit va 96-bitli *nonse*ni, shuningdek bitta doimiy qiymatni (0xFFFFFFFE) qabul qiladi va kerakli uzunlikdagi kalit oqimini generatsiya qilib, uni ochiq matnni shifrlash uchun qo‘llaydi. Algoritmning batafsil tavsifi [12] ishda berilgan.

XULOSA

Ushbu maqolada chuqur o‘rganish (deep learning) texnikalarining oqimli shifrlash algoritmlarini tahlil qilishdagi imkoniyatlari nazariy asoslangan holda o‘rganildi va keng qamrovli eksperimental tajribalar orqali tasdiqlandi. An’anaviy kriptotahlil usullari ko‘p hollarda murakkab matematik modellarga, yuqori hisoblash quvvatiga va oldindan xususiyatlarni ajratish jarayonlariga tayanishi sababli amaliy qo‘llanilishda cheklovlarga ega. Chuqur o‘rganish esa xom keystream ma’lumotlaridan o‘z-o‘zidan mazmunli xususiyatlarni aniqlash qobiliyati bilan ushbu jarayonni sezilarli darajada soddalashtiradi.

Olib borilgan tadqiqot natijalari shuni ko‘rsatdiki, deep learning asosidagi "qora quti" modeli oqimli shifrlarda ehtimoliy statistik og‘ishlarni (bias) aniqlashda samarali vosita bo‘la oladi. RC4 oqimli shifriga nisbatan o‘tkazilgan tajribalar neyron tarmoq orqali baytlar ehtimoli bo‘yicha mavjud og‘ishlarni ishonchli tarzda aniqlash mumkinligini ko‘rsatdi. Biroq RC4A, Trivium va TRIAD algoritmlarida bunday og‘ishlarning kuzatilmaganligi ushbu shifrlagichlarning yuqori darajadagi tasodifiylikka ega ekanini yana bir bor tasdiqlaydi.

Shuningdek, tadqiqot deep learning’ning kriptotahlil sohasidagi dolzarbligini isbotladi: neyron tarmoqlar klassik matematik usullar bilan aniqlash qiyin bo‘lgan nozik statistik farqlarni anglay oladi. So‘nggi yillardagi ilmiy adabiyotlar tahlili ham ushbu yondashuvning differensial kriptoanaliz, yon kanal tahlili va blokli shifrlarni qisqartirilgan roundlarda buzish kabi murakkab vazifalarda ham samarali ishlayotganini ko‘rsatadi.

Umuman olganda, maqolada taklif etilgan yondashuv kriptotizimlarning xavfsizligini baholashda chuqur o‘rganish usullarining yangi istiqbollarini ochib beradi. Olingan natijalar kelajakda:

- murakkab oqimli shifrlarda yashirin biaslarni aniqlash,
- neyron tarmoqlarni kriptoalgoritmlar barqarorligini baholash mezoni sifatida qo‘llash,

- yangi yengil vaznli shifrlash algoritmlarining xavfsizlik darajasini avtomatik tahlil qilish

kabi yo‘nalishlarda ilmiy tadqiqotlar olib borish imkonini yaratadi.

Shu tariqa, chuqur o‘rganish texnologiyalarining kriptotahlildagi roli tobora ortib borayotgani, ularning kelajak kriptografik xavfsizlik tizimlarida muhim o‘rin egallashi kutilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. Bahdanau, D.; Cho, K. & Bengio, Y. Neural machine translation by jointly learning to align and translate. arXiv preprint arXiv:1409.0473, 2014, https://arxiv.org/ abs/1409.0473 [Accessed on 01 Aug 2020].

2. Chen, C.; Seff, A.; Kornhauser, A. & Xiao, J. Deepdriving: Learning affordance for direct perception in autonomous driving. In Proceedings of the International Conference on Computer Vision, IEEE, 2015, pp. 2722-2730. doi: 10.1109/iccv.2015.312

3. Deng, L. & Yu, D. Deep learning: methods and applications. Foundations and trends in signal processing, Now Publishers Inc. Hanover, MA, USA, 2014, 7(3–4), pp. 197-387. doi: 10.1561/9781601988157

4. Rivest, R.L. Cryptography and machine learning. In Proceedings of the International Conference on the Theory and Application of Cryptology, Springer, Berlin, Heidelberg, 1991, pp. 427-439. doi: 10.1007/3-540-57332-1_36

5. Abadi, M. & Andersen, D.G. Learning to protect communications with adversarial neural cryptography. arXiv preprint arXiv:1610.06918, 2016, https://arxiv.org/ abs/1610.06918 [Accessed on 31 July 2020].

6. Hesamifard, E.; Takabi, H. & Ghasemi, M. Cryptodl: Deep neural networks over encrypted data. arXiv preprint arXiv:1711.05189, 2017, https://arxiv.org/abs/1711.05189 [Accessed on 12 July 2020]. doi: 10.1145/3292006.3300044

7. Picek, S.; Samiotis, I.P.; Kim, J.; Heuser, A.; Bhasin, S. & Legay, A. On the performance of convolutional neural networks for side-channel analysis. In Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering, Springer, Cham, 2018, pp. 157-176.

8. Wang, H. Side-channel analysis of aes based on deep learning. https://www.diva-portal.org/smash/get/diva2:1325691/FULLTEXT01.pdf, 2019 [Accessed on 07 Aug 2020].

9. Gohr, A. Improving attacks on round-reduced speck32/64 using deep learning. In Proceedings of Annual International Cryptology Conference, Springer, 2019, pp. 150–179. doi: 10.1007/978-3-030-26951-7_6

10. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B. & Wingers, L. The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptol. ePrint Arch., 2013, p.404, https://eprint.iacr.org/2013/404. pdf [Accessed on 07 Aug 2020].

11. Baksi, A.; Breier, J.; Dong, X. & Yi, C. Machine learning assisted differential distinguishers for lightweight ciphers. IACR Cryptol. ePrint Arch., 2020, p.571, https:// eprint.iacr.org/2020/571.pdf [Accessed on 14 Oct 2020].

12. Jain, A.; Kohli, V. & Mishra, G. Deep learning based differential distinguisher for lightweight cipher PRESENT. Cryptology ePrint Archive, Report 2020/846. https:// eprint.iacr.org/2020/846. [Accessed on 14 Oct 2020].