KRIPTOGRAFIYA MASALALARINI YECHISHDA SUN'IY NEYRON TARMOQLARIDAN FOYDALANISH

Allanov Orif Menglimuratovich
TATU, Kiberxavfsizlik va kriminalistika kafedrasi mudiri, phd.
E-mail: orif_allanov@mail.ru

Saparbayeva Munira Muratbay qizi
TATU magistranti

ANNOTATSIYA

Ushbu maqolada kriptografik shifrlash algoritmlarini bardoshliligini yanada barqarorlashtirish uchun sun'iy neyron tarmoqlaridan foydalanishning dolzarbligi ko'rib chiqilgan.

Kalit so'zlar: Kriptografiya, neyron, sun'iy, tarmoq, daraxt, kalit, kalit, kriptologiya,

Kriptografiya bu maxfiylik, ma'lumotlar yaxlitligi, ob'ektlarning autentifikatsiyasi va ma'lumotlarning kelib chiqishi autentifikatsiyasi kabi axborot xavfsizligining aspektlarini matematik usullardan foydalangan holda himoyalashni o'rganadi. Kriptografiyaning asosiy maqsadi ikki yoki undan ortiq shaxslarga himoyalanmagan kanal orqali raqib nima haqida gaplashayotganini tushunmaydigan tarzda muloqot qilish imkoniyatini berishdir. Kriptografiya muhim soha bo'lib, ko'plab ijtimoiy dasturlarda mavjud. Ayni paytda shifrlash va autentifikatsiya texnologiyalari butun dunyo bo'ylab xavfsizlik, harbiy va sohadan tortib elektron tijorat va bank ishi kabi davlat xizmatlarida ko'proq foydalanilmoqda.

Kompyuter texnologiyalari rivojlanib kriptografiyaga bo'lgan extiyoj borgan sari ortib bormoqda bu esa o'z o'rnida kriptografiyani tadqiq qilish va yanada mukammalroq shifrlash algoritmlarini ishlab chiqish va ularni amaliyotga tatbiq etishni taqozo etmoqda.

Kriptografik akslantirishlarni sun'iy neyron tarmoqalaridan foydalangan holda amalga oshirish kriptotizimni bardoshliligini oshiradi. Sun'iy neyron tarmoqlaridan kriptografiyaning har ikkala sohasi kriptologiya va kriptoanalizda ham barqaror foydalanish mumkin.

Kriptografiya elektron raqamli imzo, abonentlarni identifikatsiya qilish va autentifikatsiya qilish, kalitlarni xavfsiz saqlash va boshqalar kabi tizim xavfsizligini ta'minlashning mahalliy va taqsimlangan vositalarini taqdim etadi. Bu jarayonlarni

amalga oshirishda bir qancha muammolar kelib chiqadi ushbu muammolarni hal qilishda sun’iy neyron tarmoqlardan foydalanish muammoni mukammal hal etish imkonini beradi. Neyron tarmoqlarning o‘z-o‘zini o‘rganish va stokastik xatti-harakatlari g‘oyalari va shunga o‘xshash algoritmlar kriptografiyaning turli jihatlari uchun ishlatilishi mumkin. Masalan, ochiq kalitli kriptografiya, xeshlash yoki psevdotasodifiy sonlarni genaratsiyalash va kalitlarni tarqatish muammosini hal qilish [3].

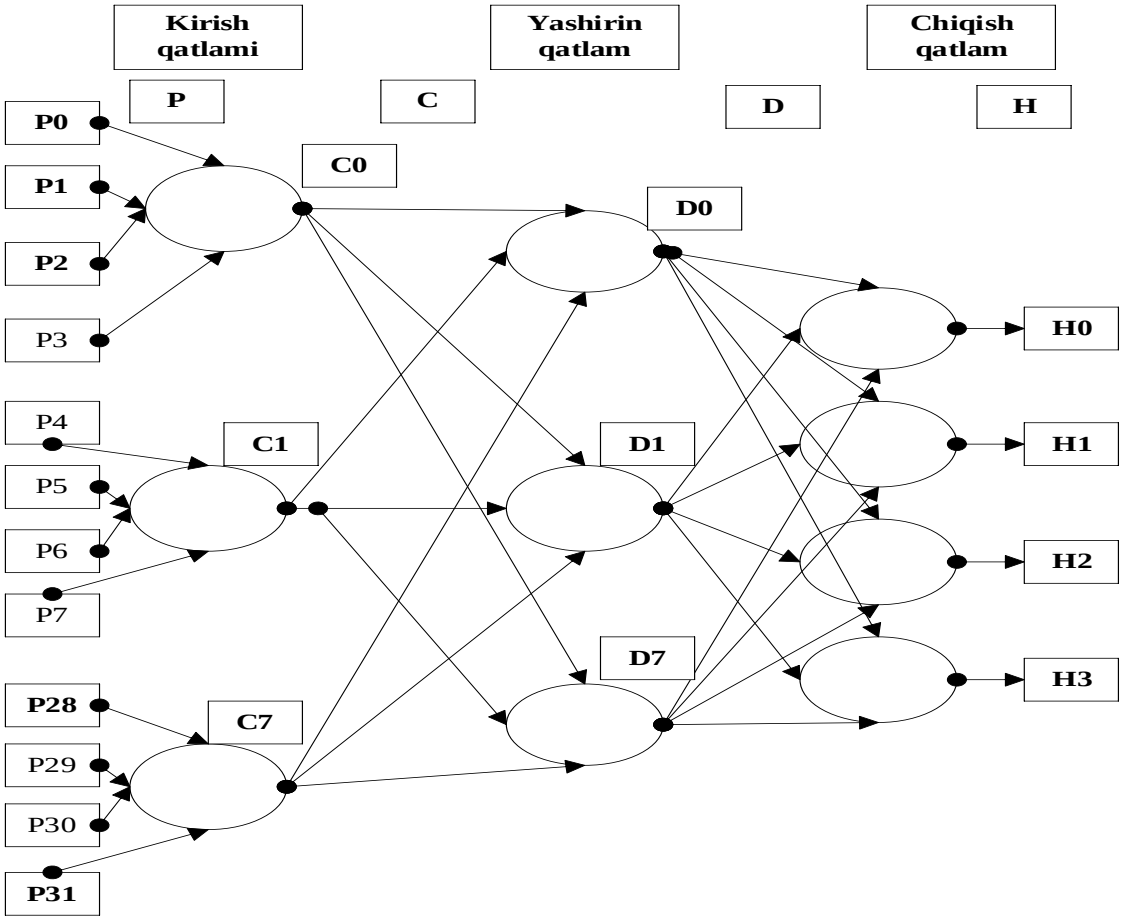
An’anaviy kriptografik tizimlar uchun kalit uzunligini oshirish orqali protokol xavfsizligini yaxshilashimiz mumkin. Neyron kriptografiyasida neyron tarmoqlarni chuqur o‘qitish orqali yaxshilash mumkin. Ushbu parametrni o‘zgartirish muvaffaqiyatli hujumning narxini oshiradi, foydalanuvchilar uchun tizim xavfsizligini ta’minlaydi. Shuning uchun neyron kalit almashinuvining xavfsizligini buzish yuqori murakkablik sinfiga tegishli masala hisoblanadi.

Ma’lumki, sun’iy neyron tarmoqlari bir nechta qatlamlardan iborat, bitta yashirin qatlam bilan to‘g‘ridan-to‘g‘ri tarqaladigan sun’iy neyron tarmoqlar har qanday funksiyaning yaqinlashish darajasi bo‘yicha pastki chegaraga ega. Agar bir nechta yashirin qatlam ishlatilsa, bu chegara ko‘tarilishi mumkin. Bu holat kriptologiyada uchraydigan diskret tuzilmalarda kuchli hisoblash vositasini joriy qilish imkonini beradi [2].

Neyron tarmoqlarini kriptografiyadaning bir qancha usullarida qo‘llash mumkin. Masalan, Tree Parity Machine (TPM) neyron kriptografiyasi uchun eng keng tarqalgan neyron tarmoq topologiyasidir bo‘lib uni kalit almashishda qo‘llash mumkin. U K×N kirish neyronlari, K yashirin neyronlar va bitta chiqish neyronlari O dan iborat. Neyron kriptografiyasining asosi o‘zaro o‘rganishdan keyin sinxronlasha oladigan ikkita bir xil sun’iy neyron tarmoqlardan (SNT) foydalanadi. Boshida har bir TPM maxfiy bo'lgan og‘irliklarning (w_{kj}) tasodifiy qiymatlarini yaratadi. O'quv jarayoni ikkala TPM uchun bir xil tasodifiy kirishlarni yaratishdan, so‘ngra har bir TPMdan chiqishlarni hisoblash va ularni o‘zaro solishtiriladi [1].

TPM larni o‘rganish ikkala TPM ning chiqish bitlarini solishtirish orqali amalga oshiriladi, bunda kirish vektori x ikkala TPM uchun teng bo'ladi. Ikki TPMni sinxronlashtirish uchun turli xil o'rganish qoidalaridan foydalanish mumkin.

Shuningdaek sun’iy neyron tarmoqlari xeshlash algoritmlarida qo‘llash mumkin. sun’iy neyron tarmoqlari yordamida xeshlash algoritmlarini yaratishga bag'ishlangan bir qator ilmiy ishlar mavjud.



1-rasm. Hesh funktsiyani qurish uchun ishlatiladigan sun’iy neyron tarmoq modeli

Hesh funksiyada ishlatiladigan ANN 1-rasmda ko'rsatilgan. Uch qavatli beshta neyron tarmog‘i va xaotik xaritalash qo‘llaniladi. Qoida tariqasida xaotik xaritalash sifatida boshqaruvchi parametrga ega bo‘lgan qismli chiziqli funktsiyalarning bir qator takrorlanishi qo‘llanilgan. Displeyning tasodifiyligi parametr qiymati bilan belgilanadi. Tadqiqotlar shuni ko'rsatadiki, xaotik xaritalashning takrorlanish sonini to'g'ri tanlash bilan, kirish parametrlarining ozgina o'zgarishi bilan funktsiyaning chiqish qiymati juda boshqacha bo'ladi. Yuqoridagi rasmda neyronlarning yashirin qatlamida xash funktsiyasini hisoblash uchun zarur bo'lgan operatsiyalar sonini kamaytirish uchun xaotik xaritalash takrorlanmaydi va T ($T \geq 50$) takrorlashlar kirish va chiqish qatlamlarida bajariladi. Hash algoritmi yuqorida tavsiflangan sun’iy neyron tarmog‘i va kalit generatori asosida qurilgan. Kalit generatori foydalanuvchi kalitini har bir qatlam uchun og'irliklar, ofsetlar va boshqarish parametrlari to‘plamiga o'zgartiradi. Algoritm o'zboshimchalik uzunligidagi ma'lumotlarni 128 bitli xash qiymatiga o'zgartiradi. Buning uchun ma’lumotlar avval quyidagi neytral algoritmga binoan neyron tarmog'ining kiritilishiga beriladigan 1024-bitli blokning ko'paytmasiga erishiladi: bitta birlikni va qolgan nollarni oxirgi ko'p bo'lmagan blokga qo'shiladi. Shundan so'ng, har bir blok neyron tarmoqning kirish qismiga beriladi[5].

Natija quyidagi formula yordamida hisoblanadi:

$H_M=K_{M_{n-2}} + K_{M_{n-1}} = (K_{M_{n-3}} + K_{M_{n-2}}) + H_{M_{n-1}} = ---- = (K + H_{M_0}) + H_{M_1} + \ldots. H_{M_{n-1}}$

Yuqorida keltirib o‘tilgan ma’lumotlardan kelib chiqib shuni aytish mumkinki sun’iy neyron tarmoqlar kriptografiya sohasiga dadil qadamlar qo‘yib kelmoqda. Neyron tarmoqlardan nafaqat kriptografiyaning istalgan yo‘nalishida balki har qanday boshqa sohada ham qo‘llash mumkin. Ma’lumotlarni shifrlash va ularni kanallar orqali uzatishda o‘zaro bog‘langan ikki neyron tarmoq yaratish, hamda ikki neyron tarmoqni shunday o‘rgatish lozimki ularni bir birlaridan boshqa hech qanday tizim tushuna olmasin. Ma’lumot ikki neyron tarmoq o‘rtasida faqat ulargagina ma’lum bo‘lgan protokol orqali almashiniladi. Protokol neyron tarmoqlar bir-birni o‘rgatish mobaynida vujudga keladi. Neyron tarmoqning kiruvchi oqimiga ochiq ma’lumot taqdim etiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. Kinzel W., Kanter I. Interacting neural networks and cryptography // Advances in Solid State Physics. Springer Verlag, 2002. V. 42. P. 383–391.
2. “Use of Artificial Neural Networks in Cryptography” Ing. Martin Javurek, Ing. Michal Turčaník, PhD, doc. Ing. Marcel Harakal, PhD, Ing. Miloš Očkay, PhD, 02 may 2019.
3. Бекмуратов Т. Ф., Мухамедиева Д.Т. Теория, методы и алгоритмы синтеза нейро-нечетких моделей принятия решений при интеллектуальном анализе данных. Ташкент-2016г.
4. https://ru.wikipedia.org/wiki/Искусственная_нейронная_сеть
5. https://ru.wikipedia.org/wiki/Нейронная_сеть