KRIPTOANALIZ USULLARINING ZAMONAVIY AXBOROT XAVFSIZLIGIDAGI O‘RNI

Fotimaxon Temirxonova Xomidxon qizi
O‘zbekiston Milliy universiteti Jizzax filiali
fotimaxon0404@gmail.com

Annotatsiya. Raqamli texnologiyalar va kiberhujumlar ko'lamining keskin ortib borishi fonida shifrlash tizimlarining ishonchliligini baholashda kriptoanalizning o'rni beqiyosdir. Kvant kompyuterlari va sun'iy intellektning jadal rivojlanishi axborot xavfsizligida qo'llaniluvchi an'anaviy kriptografik algoritmlarni zaiflashtirib borayotgani ushbu tadqiqotning dolzarbligini belgilab beradi. Maqolaning maqsadi — zamonaviy axborot xavfsizligi tizimlarida qo'llanilayotgan ilg'or kriptoanaliz usullarini batafsil tahlil qilish hamda ularning xalqaro himoya standartlariga (AES, RSA) ta'sirini ilmiy va amaliy jihatdan baholashdan iborat. Tadqiqot jarayonida mantiqiy, tizimli va qiyosiy tahlil, an'anaviy statistik kriptoanaliz (chiziqli, differensial, chastotali tahlil), shuningdek, mashinali o'rganish modellarini kriptografik hujumlarga tatbiq etish kabi metodlardan foydalanildi. Olib borilgan izlanishlarning asosiy natijasi sifatida standart shifr turlarining murakkab tahliliy hamda neyron-yordamli statistik hujumlarga bardoshlilik darajasi tizimlashtirildi. Tahlillar shuni ko'rsatdiki, gibrid kriptoanaliz usullari shifr kalitini tiklash va qidirish maydonini qisqartirish jarayonini bir necha barobar tezlashtiradi. Maqolaning ilmiy yangiligi shundan iboratki, unda klassik statistik kriptoanaliz usullari va zamonaviy chuqur o'rganish (deep learning) texnologiyalarining integratsiyasi axborot xavfsizligi mezonlarini qanday o'zgartirishi ilmiy asoslandi. Shuningdek, xavfsizlik tizimlarini modernizatsiya qilish va post-kvant davriga o'tish bo'yicha konseptual yechimlar taklif etildi.

Kalit so‘zlar: kriptoanaliz, axborot xavfsizligi, statistik hujumlar, chiziqli kriptoanaliz, differensial kriptoanaliz, AES, RSA, chuqur o'rganish (deep learning).

Kirish. Raqamli iqtisodiyotning jadal rivojlanishi, bulutli texnologiyalar, narsalar interneti (IoT) va elektron davlat xizmatlarining keng joriy etilishi davrida zamonaviy axborot tizimlarida axborot xavfsizligining ahamiyati mislsiz darajada oshdi. Har qanday davlat, korporatsiya va shaxsning maxfiy ma'lumotlarini ruxsatsiz kirish, o'zgartirish yoki o‘g‘irlashdan himoya qilish bugungi kunning eng dolzarb masalasiga aylangan. Axborotning maxfiyligi, butunligi va ochiqligini ta'minlamasdan turib, raqamli infratuzilmaning barqaror ishlashini kafolatlab bo'lmaydi.

Ushbu xavfsizlikni ta'minlashning asosi hisoblangan kriptografiya va kriptoanaliz tushunchalari axborotni himoya qilish tangasining ikki tomonidir. Kriptografiya — bu matematik algoritmlar yordamida ochiq ma'lumotlarni shifrlash, ishonchli aloqa kanallarini yaratish va ularni ruxsatsiz shaxslar tushunolmaydigan holatga keltirish fanidir. Kriptoanaliz esa — shifrlangan ma'lumotlarni (shifr matnni) ularning maxfiy kalitini bilmasdan turib o'qish, shuningdek, shifrlash algoritmlari, protokollari va dasturiy ta'minotlaridagi arxitekturaviy yoki matematik zaifliklarni topish usullarini o'rganuvchi sohadir.

Bugungi kunda jahon axborot makoni jiddiy kiberxavfsizlik muammolari bilan to‘qnash kelmoqda. Hisoblash quvvatlarining keskin ortishi, sun'iy intellekt (AI) texnologiyalarining kiberhujumlarni avtomatlashtirishda qo‘llanilishi va kelajakda an'anaviy asimmetrik shifrlarni (masalan, RSA) sanoqli daqiqalarda buza oladigan kvant kompyuterlarining yaratilishi (Shor algoritmi xavfi) mavjud axborot himoyasi tizimlari oldiga ulkan tahdidlarni qo‘ymoqda. Bunday murakkab sharoitda faqatgina "kuchli qulflar" yaratishning o‘zi yetarli emas.

Aynan shu nuqtada kriptoanaliz usullarining zarurligi namoyon bo‘ladi. Hech bir shifrlash standarti (masalan, AES) to u yillar davomida eng kuchli kriptoanalitik hujumlarga (chiziqli, differensial yoki algebraik tahlillarga) bardosh bermagunicha xavfsiz deb tan olinmaydi.Yuqoridagilardan kelib chiqib, ushbu tadqiqotning maqsadi — zamonaviy axborot xavfsizligini ta'minlashda qo‘llanilayotgan qat'iy va intellektual kriptoanaliz usullarini tizimli o‘rganish hamda ularning shifrlash standartlarini takomillashtirishdagi tutgan o‘rnini ilmiy-amaliy jihatdan asoslashdan iborat.

Ushbu maqsadga erishish uchun quyidagi vazifalar belgilab olindi:

Kriptoanalizning an'anaviy va zamonaviy usullarining mexanizmlari hamda evolyutsiyasini tahlil qilish.

Keng tarqalgan axborot xavfsizligi algoritmlarining (RSA, AES, DES) turli xil kriptoanalitik hujum modellariga chidamlilik darajasini baholash;

Adabiyotlar tahlili. Zamonaviy ochiq kalitli kriptografiyaga Whitfield Diffie va Martin Hellman o‘zlarining 1976-yildagi inqilobiy ishlari orqali asos solganlar. Ularning kalit almashish protokoli axborotni xavfsiz uzatishda asimmetrik yondashuvni boshlab berdi. Bunga asoslanib, 1977-yilda Ronald Rivest, Adi Shamir va Leonard Adleman tomonidan yaratilgan RSA algoritmi butun jahon axborot xavfsizligining amaliy standartiga aylandi. Ta'kidlash joizki, Adi Shamir nafaqat himoya tizimini yaratishda, balki Eli Biham bilan birgalikda differensial kriptoanaliz usulini ishlab chiqish orqali shifrlarni buzish (zaifligini tekshirish) sohasida ham ulkan ilmiy burilish yasagan. U o‘z ishlari orqali xavfsizlik faqat matematikaga emas, balki tizimning to‘g‘ri joriy etilishiga bog'liqligini isbotlagan. Shuningdek, William Stallings o‘zining ilmiy asarlarida ("Cryptography and Network Security") simmetrik va asimmetrik shifrlar (AES, DES, RSA) xavfsizligi, tarmoq hujumlari hamda chiziqli va differensial kriptoanaliz mexanizmlarini tizimli tahlil qilib bergan.

AI va Mashinali o'rganish (Machine Learning) xavfi. Zamonaviy kriptoanalizga sun'iy intellekt (AI) va chuqur o'rganish (Deep Learning) texnologiyalarining kirib kelishi "qilich va qalqon" kurashini butunlay boshqa bosqichga olib chiqdi. Ilgari faqat inson aqli va an'anaviy matematik tahlil orqali yillar davomida izlanadigan statistik og'ishlar (masalan, chiziqli va differensial kriptoanalizda) bugungi kunda mashinali o‘rganish modellari yordamida tezroq va avtomatik ravishda aniqlanmoqda. Bu usul ilm-fanda "Neyron-yordamli statistik hujum" (Neural-aided statistical attack) deb ataladi.

IoT (Narsalar interneti) va Yon-kanal (Side-channel) hujumlari Mikrokontrollerlar va aqlli qurilmalarning keng tarqalishi axborot xavfsizligida o‘ta zaif nuqtalarni yuzaga keltirdi. Aksariyat IoT qurilmalari cheklangan hisoblash quvvati va xotiraga ega bo'lganligi sababli murakkab, kuchli shifrlash standartlarini ishlata olmaydi.

Hozirgi kungacha ushbu fizik zaifliklarga qarshi universal apparat-dasturiy himoya standarti ishlab chiqilmagan. Katta ma'lumotlar (Big Data) va Bulutli hisoblash muammolari. Katta hajmdagi ma'lumotlarni bulutli serverlarda shifrlangan holda ishonchli saqlash va qayta ishlash ham jiddiy muammo bo‘lib qolmoqda.

Kriptoanaliz tushunchasi. Kriptoanaliz (yunoncha kryptos – yashirin, analyein – ochish, tahlil qilish) — bu shifrlangan ma'lumotlarning (shifr matnning) maxfiy kalitini bilmasdan turib ochiq matnni o‘qish, tizimning yashirin jihatlarini aniqlash va kriptografik algoritmlarning xavfsizlik darajasini buzish usullarini o‘rganuvchi fandir. U asosan matematik, statistik va mantiqiy tahlil usullariga tayanadi hamda axborot tizimlarining xavfsizlik qobig'ini chetlab o‘tish imkoniyatlarini tadqiq qiladi.

Kriptografiya va kriptoanaliz o‘rtasidagi bog‘liqlik Kriptografiya (axborotni shifrlash orqali himoya qilish) va kriptoanaliz (ushbu himoyani buzish tahlili) bir-biri bilan chambarchas bog'liq bo‘lib, ular birgalikda yagona kriptologiya fanini tashkil etadi. Kriptotizimlarning xavfsizlik modeli. Zamonaviy kriptotizimlarning xavfsizlik modeli fundamental Kerkgof (Kerckhoffs) tamoyiliga asoslanadi.

Bu tamoyilga ko‘ra, "kriptotizimning xavfsizligi uning algoritmik sir saqlanishiga emas, balki faqatgina kalitning maxfiyligiga bog'liq bo‘lishi kerak". Ya'ni, hujumchi shifrlash dasturining qanday ishlashini (kodini) to‘liq bilsa ham, maxfiy kalitsiz ma'lumotni o‘qiy olmasligi shart. Shunga ko‘ra, kriptotizimlarning xavfsizlik imkoniyatlarini sinash uchun hujumchiga ma'lum bo‘lgan axborot hajmiga qarab to‘rtta asosiy model farqlanadi:

1. Faqat shifr matnli hujum (Ciphertext-only attack).
2. Ma'lum ochiq matnli hujum (Known-plaintext attack).
3. Tanlangan ochiq matnli hujum (Chosen-plaintext attack).
4. Tanlangan shifr matnli hujum (Chosen-ciphertext attack).

Axborot xavfsizligida kriptoanalizning vazifalari. Kriptoanaliz axborot xavfsizligida quyidagi o'ta muhim vazifalarni bajaradi. Algoritmlarni audit qilish va sertifikatlash.

Zaifliklarni proaktiv aniqlash. Standartlarni yangilashga asos yaratish. Favqulodda vaziyatlarda kirishni ta'minlash.

Kriptoanaliz usullarining turlari.

1. Brute Force (To‘liq qidiruv) usuli. Hujumchi to‘g‘ri kalit topilmagunicha mavjud bo‘lgan barcha kalit kombinatsiyalarini birma-bir tekshirib chiqadi. Bu algoritmning matematik zaifligiga emas, balki hisoblash quvvatiga tayanadi.Afzalligi sifatida algoritm qanday bo‘lishidan qat'i nazar, agar yetarli vaqt va hisoblash quvvati bo‘lsa, usulning natija berishi 100% kafolatlangan. Kamchiligi zamonaviy uzun kalitli shifrlarda bu usul o‘ta samarasiz. Barcha kombinatsiyalarni tekshirish uchun hatto superkompyuterlarga ham milliardlab yillar kerak bo‘ladi. Qisqa parollarni buzish, eskirgan shifrlash standartlarini tahlil qilish, shuningdek, oflayn rejimdagi arxiv yoki hujjatlar parolini ochish kabi holatlarda qo‘llaniladi.

.2. Statistik kriptoanaliz. Tabiiy tillardagi ma'lumotlarning va shifr matnning uchrashish chastotasini hamda statistik qonuniyatlarini tahlil qilishga asoslanadi. Afzalligi juda kam hisoblash quvvati talab qiladi. Klassik shifrlarga nisbatan o‘ta tezkor va aniq ishlaydi.Kamchiligi sifatida zamonaviy axborot xavfsizligi algoritmlariga nisbatan butunlay yaroqsiz holati keltiriladi. Tarixiy va klassik shifrlarni buzish, zaif tasodifiy sonlar generatorlarini tekshirish va yopiq (xususiy) zaif algoritmlarni tahlil qilishda qo‘llaniladi.

2. Differensial kriptoanaliz *Tanlangan ochiq matnli hujum* turiga kiradi. Ikkita ochiq matn o‘rtasidagi kichik farq shifrlash bosqichlaridan o‘tgandan so‘ng shifr matnlar o‘rtasida qanday farqni yuzaga keltirishini tahlil qiladi. Uning afzalligi blokli shifrlarni buzishda kalit qidirish maydonini *Brute Force* usuliga qaraganda bir necha barobar qisqartirib beradi. Kamchiligi hujumchi ixtiyoridagi juda ko‘p miqdordagi maxsus tanlangan ochiq matn va shifr matn juftliklari bo‘lishini talab qiladi, bu esa real sharoitda doim ham imkoni bo‘lavermaydigan holatdir. Simmetrik blokli shifrlarni va ba'zi xesh funksiyalarni tahlil qilish hamda yangi algoritmlar yaratishda ularning mustahkamligini sinash kabi sohalarda qo‘llaniladi

Chiziqli kriptoanaliz. Ma'lum ochiq matnli hujum turiga kiradi. Ochiq matn,shifr matn va maxfiy kalit bitlari o‘rtasidagi ehtimoliy chiziqli munosabatlarni qidirishga asoslanadi. Afzalligi differensial tahlildan farqli o‘laroq, hujumchidan ochiq matnlarni maxsus tanlashni talab qilmaydi, shunchaki tizimdan o‘tgan ixtiyoriy matnlar juftligi yetarli hisoblanadi. Bu reallikka yaqinroqdir. Kamchiligi statistik og'ishlarni (bias) aniq hisoblash uchun nihoyatda katta hajmdagi ma'lum matnlar to‘plamini talab qiladi. Asosan DES va unga o‘xshash blokli shifrlar, shuningdek, oqimli shifrlarning ishonchliligini baholash kabi holatlarda qo‘llaniladi

Xesh funksiyalar kriptoanalizi. Axborotning butunligini ta'minlovchi xesh funksiyalarga (MD5, SHA) qarshi qaratilgan bo‘lib, turli xil ochiq matnlarning bir xil xesh qiymatga ega bo‘lish holatini (kolliziya – *collision attack*) yoki berilgan xeshdan asl matnni topishni (Tug'ilgan kun xavfi – *Birthday attack*) o‘rganadi. Afzalligi agar kolliziya topilsa, hujumchi tizimdagi asl hujjat yoki ruxsatnomani soxtasiga (asli bilan bir xil xeshga ega bo‘lgan zararli faylga) almashtirib qo‘yishi mumkin. Kamchiligi zamonaviy xesh funksiyalarda (SHA-256, SHA-3) kolliziya topish matematik jihatdan o‘ta murakkab va hozircha amaliy jihatdan imkonsiz hisoblanadi.

Yon kanal (Side-channel) hujumlari. Ushbu usul matematik algoritmdagi xatolarni qidirmaydi, balki shifrlash jarayonini amalga oshirayotgan qurilmaning *fizik xususiyatlarini* nishonga oladi. Shifrlash vaqtida qurilma sarflayotgan elektr toki tebranishlari (DPA), operatsiyani bajarish uchun ketgan vaqt (Timing attack) yoki tarqatayotgan elektromagnit nurlari tahlil qilinib, kalit bitlari aniqlanadi.Afzalligi istalgancha kuchli matematik algoritm (hatto AES-256 yoki RSA-4096) bo‘lishiga qaramay, ularni apparat darajasida chetlab o‘tib, maxfiy kalitni qisqa vaqt ichida o‘g‘irlash imkonini beradi.Kamchiligi esa hujumchidan qurilmaning yonida bo‘lishni yoki unga jismoniy ulana olishni talab qiladi.

Zamonaviy kriptotizimlar xavfsizligini baholash. Bugungi kunda jahon axborot xavfsizligi arxitekturasini ushlab turgan asosiy algoritmlar misolida kriptoanalizning xavfsizlikka ta'sirini quyidagicha baholash mumkin:

1. AES (Advanced Encryption Standard) xavfsizligini baholash. AES hozirgi kunda dunyodagi eng keng tarqalgan simmetrik blokli shifrlash standarti hisoblanadi. AES aynan shu klassik statistik hujumlarga qarshi immunitetga ega qilib loyihalashtirilgan. Uning matematik tuzilmasiga hozirgacha hech qanday amaliy halokatli hujum topilmagan. Shunday bo‘lsa-da, AES tizimlari yon-kanal (Side-channel) hujumlariga o‘ta zaifdir.

2. RSA (Rivest-Shamir-Adleman) xavfsizligini baholash. RSA raqamli imzolar va kalit almashish protokollarida keng qo‘llaniluvchi asimmetrik algoritm bo‘lib, uning xavfsizligi juda katta ikkita tub sonni ko‘paytuvchilarga ajratishning (faktoring) matematik murakkabligiga asoslanadi. RSA matematik jihatdan ishonchli bo'lsa-da, uning amaliyotga noto‘g'ri joriy etilishi kriptoanalitiklar uchun oson nishon bo‘ladi. Agar RSA shifrlashda tasodifiy to‘ldirma (OAEP padding) ishlatilmasa, u tanlangan shifr matnli hujumlarga (masalan, Bleichenbacher hujumi) darhol dosh bermay qoladi. Hozirda RSA o‘rnini bosuvchi post-kvant algoritmlarini yaratish sohaning asosiy maqsadiga aylangan.

3. SHA (Secure Hash Algorithm) xavfsizligini baholash. SHA oilasi ma'lumotlarning butunligini tasdiqlash, parollarni xesh ko‘rinishida saqlash va raqamli imzolarda ishlatiladi. Kriptoanaliz ta'siri kriptoanalitiklar differensial tahlil usullarini xesh funksiyalarga moslashtirish orqali avvalgi avlod standartlari bo‘lgan MD5 va SHA-1 algoritmlarida kolliziya (collision) xatoliklarini topishga muvaffaq bo‘lishdi. Kvant kompyuterlari xesh funksiyalarga RSA kabi halokatli ta'sir ko‘rsata olmaydi, faqat xesh uzunligini kattalashtirish (masalan, SHA-256 o'rniga SHA-512 ishlatish) yetarli mudofaa hisoblanadi.

Kriptoanaliz usullarining axborot xavfsizligidagi roli

Ko‘pchilik hollarda kriptoanaliz faqatgina xakerlar va jinoyatchilarning axborotni o‘g‘irlash quroli sifatida tushuniladi. Kriptoanaliz usullarisiz xavfsizlik tizimlarining haqiqiy holatini baholab bo‘lmaydi. Uning bugungi kundagi o‘rni quyidagi to‘rtta asosiy yo‘nalishda yaqqol namoyon bo‘ladi:

1. Kriptotizimlarni tekshirish. 2. Xavfsizlik darajasini aniqlash.3. Yangi shifrlash algoritmlarini yaratish. 4. Kiberhujumlarni aniqlash va oldini olish.

Tadqiqot natijalari va muhokama

Olib borilgan tadqiqotlar shuni ko‘rsatmoqdaki, balki real vaqt rejimida ishlovchi amaliy xavfsizlik mexanizmidir. Kriptoanaliz metodlarining tahlili, ularning amaliyotga joriy etilishi va saqlanib qolayotgan muammolar bo‘yicha quyidagi natijalar olindi:

1. Kriptoanaliz metodlarining samaradorligi. Tadqiqot natijalari an'anaviy va zamonaviy kriptoanaliz usullarining samaradorligida katta farq borligini ko‘rsatdi:

Matematik usullarning cheklanganligi. AES-256, RSA-2048 yoki SHA-3 kabi zamonaviy standartlarga nisbatan Brute force (to‘liq qidiruv), chiziqli va differensial kriptoanaliz usullari sof matematik nuqtai nazardan o‘z samaradorligini yo‘qotgan. Hujumchilar algoritmning o‘zini emas, balki u ishlayotgan mikrokontroller (dasturiy muhit) zaifliklaridan foydalanib, kalitlarni muvaffaqiyatli ajratib olmoqdalar. Bu esa xavfsizlikni faqat matematik modellar bilan o‘lchash xato ekanligini isbotlaydi.

2. Zamonaviy kiberxavfsizlik tizimlarida qo‘llanilishi.

Protokollarni takomillashtirish: TLS 1.2 protokolida kriptoanalitiklar tomonidan topilgan zaifliklar (masalan, POODLE, BEAST hujumlari) natijasida, bugungi kunda internet trafigini himoyalovchi ancha xavfsiz va tezkor TLS 1.3 standarti ishlab chiqildi va ommaviy joriy etildi.

Zararli tarmoq trafigini tahlil qilish. Kiberxavfsizlik operatsion markazlari (SOC) tarmog'ida ma'lumotlar shifrlangan bo‘lsa ham, paketlarning uzunligi, vaqti va uchrashish chastotasini tahlil qilish (Traffic analysis) orqali yashirin botnetlar, to‘lov talab qiluvchi viruslar (Ransomware) va ma'lumotlarni sizib chiqish (Data exfiltration) holatlarini aniqlamoqda.

3. Mavjud muammolar va kelajak tahdidlari. Tadqiqotlar va adabiyotlar tahlili shuni tasdiqlaydiki, kuchli shifrlash standartlari mavjudligiga qaramay, sohada qator o‘tkir muammolar ochiq qolmoqda. Kvant apokalipsisi Kvant kompyuterlarining jadal rivojlanishi amaldagi butun ochiq kalitli infratuzilmani (PKI, RSA, ECC algoritmlarini) xavf ostiga qo‘ymoqda. "Avval o‘g‘irla, keyinroq och" (Harvest Now, Decrypt Later)

taktikasi. Kiberjinoyatchilar hozirgi kunda buzish imkonsiz bo‘lgan kuchli shifrlangan ma'lumotlarni katta hajmdagi serverlarda saqlab qo‘ymoqdalar. Maqsad — kelajakda kvant kompyuterlari yoki kuchli AI tizimlari yordamida ularning parolini ochishdir. Narsalar interneti (IoT) qurilmalarining resurslari cheklanganligi sababli ushbu muammo yanada chuqurlashmoqda.

Muhokama xulosasi. Olingan natijalar shuni ko‘rsatadiki, axborot xavfsizligida statik, o‘zgarmas himoya degan tushuncha yo‘q. Kriptoanaliz metodlari sun'iy intellekt va kvant hisoblashlari hisobiga evolyutsiya qilib borar ekan, kiberxavfsizlik tizimlari ham gibrid (ham an'anaviy, ham post-kvant) mudofaa mexanizmlariga o‘tishi shart. Xavfsizlikni ta'minlash faqatgina kuchli matematik formula bilan emas, balki apparat, dasturiy ta'minot va tarmoq darajasidagi kompleks yondashuv bilan amalga oshirilishi kerak

Xulosa. Ushbu tadqiqot doirasida zamonaviy axborot xavfsizligida kriptoanaliz usullarining tutgan o‘rni, ularning evolyutsiyasi va raqamli infratuzilmalarni himoya qilishdagi ahamiyati chuqur tahlil qilindi. Olib borilgan izlanishlar asosida quyidagi yakuniy xulosalar shakllantirildi.

Tadqiqot natijalari. Tahlillar shuni ko‘rsatdiki, AES, RSA va SHA kabi zamonaviy xalqaro shifrlash standartlari an'anaviy statistik, chiziqli va differensial kriptoanaliz hujumlariga nisbatan yuqori matematik mustahkamlikka ega. Biroq, real tizimlarning xavfsizligi faqat algoritmning mukammalligiga emas, balki uning dasturiy va apparat ta'minotidagi to‘g‘ri joriy etilishiga (implementation) bevosita bog‘liq. Kriptoanaliz usullarining ahamiyati. Kriptoanaliz fani kiberxavfsizlikning harakatlantiruvchi kuchi hisoblanadi. Usiz hech bir shifrlash tizimining ishonchliligini obyektiv baholab bo‘lmaydi. Kriptoanaliz "qilich va qalqon" kurashida ham hujum, ham mudofaa vositasi sifatida xizmat qilib, eskirgan va zaiflashgan algoritmlarni muomaladan chiqarishga hamda o‘zida hech qanday tuynuk qoldirmaydigan yangi, kuchli shifrlash arxitekturalarini yaratishga ilmiy zamin yaratadi.

Axborot xavfsizligini ta’minlashdagi roli esa zamonaviy axborot xavfsizligida kriptoanaliz raqamli tizimlarning "immun tizimi" vazifasini bajaradi. U kiberjinoyatchilar

haqiqiy hujumni amalga oshirishidan oldin tizimdagi mantiqiy, arxitekturaviy va fizik zaifliklarni proaktiv tarzda fosh etadi. Kelajakdagi tadqiqot yo‘nalishlari raqamli texnologiyalarning jadal rivojlanishini inobatga olgan holda, kelajakdagi ilmiy tadqiqotlar quyidagi ustuvor yo‘nalishlarga qaratilishi maqsadga muvofiqdir. Post-kvant kriptografiyasi (PQC).Shor va Grover algoritmlarini ishlata oladigan kvant kompyuterlari tahdidiga qarshi bardoshli bo‘lgan yangi avlod (panjaraga yoki xeshga asoslangan) shifrlash standartlarini yaratish va ularni global tizimlarga og‘riqsiz integratsiya qilish

Sun'iy intellekt va Kriptoanaliz. Neyron tarmoqlar va chuqur o‘rganish texnologiyalarini kriptoanaliz jarayonlariga joriy etish, AI yordamida ishlovchi avtomatlashtirilgan hujum va mudofaa mexanizmlarini o‘rganish.IoT qurilmalari uchun yengil kriptografiya resurslari va hisoblash quvvati cheklangan aqlli qurilmalar hamda sensorlar uchun yon-kanal hujumlariga to‘liq chidamli bo‘lgan, kam energiya sarflovchi maxsus shifrlash algoritmlarini ishlab chiqish.Axborot xavfsizligi statik jarayon emas. Axborot makonining daxlsizligini ta'minlash uchun kriptografik himoya vositalari doimiy ravishda eng ilg‘or kriptoanalitik sinovlardan o‘tkazilishi va zamon talablariga mos ravishda yangilanib borilishi hayotiy zaruratdir.

Foydalanilgan adabiyotlar

1. G‘aniyev, S.Q., Karimov, M.M., & Tashev, K.A. (2020). Axborot xavfsizligi. Darslik. Toshkent: "Aloqachi" nashriyoti. (O'zbek olimlari)

2. Aripov, M.M., & boshqalar. (2019). Axborot xavfsizligi va kriptografiya asoslari. O‘quv qo‘llanma. Toshkent: O‘zbekiston Milliy universiteti (O'zMU). (O'zbek olimlari)

3. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8-nashr). Pearson.

4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

5. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

6. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3-nashr). CRC Press.

7. inLibrary – O‘zbekiston ilmiy maqolalar bazasi. Axborot xavfsizligi va kriptotizimlar tahliliga oid maqolalar arxivi. Elektron manba:https://inlibrary.uz/

8. Splunk Inc. (2023). What is Cryptanalysis? A Detailed Introduction. Kiberxavfsizlik va axborot tahlili markazi materiallari. Elektron manba: https://www.splunk.com/en_us/blog/learn/cryptanalysis.html