

SUN'IY INTELLEKT USULLARI ASOSIDA ELEKTRON RAQAMLI IMZO ALGORITMLARINING KRIPTOGRAFIK TAHLILI

Urozova Sevinch G'ayratovna O'zbekiston Milliy Universiteti magistranti

Annotatsiya: Mazkur maqolada DSA va ECDSA elektron raqamli imzo algoritmlarining matematik asoslari, ishlash prinsiplari hamda ularning o'zaro o'xshash va farqli jihatlari tahlil qilinadi. Algoritmlarning kriptografik bardoshliligi, kalit uzunligi va hisoblash samaradorligi nuqtai nazaridan solishtiriladi. Shuningdek, ECDSA algoritmidagi tasodifiy parametr k ning takroran ishlatilishi natijasida yuzaga keladigan xavfsizlik muammosi matematik jihatdan ko'rib chiqiladi.

Bundan tashqari, maqolada sun'iy intellekt va mashinaviy o'rganish usullaridan foydalanib elektron raqamli imzolarni tahlil qilish imkoniyatlari yoritiladi. Klassifikatsiya, klasterlash va anomaliyalarni aniqlash usullari orqali katta hajmdagi ma'lumotlar orasidan yashirin zaifliklar va noodatiy holatlarni aniqlash mumkinligi asoslab beriladi.

Kalit so'zlar: DSA, ECDSA, elektron raqamli imzo, sun'iy intellekt, mashinaviy o'rganish, kriptografiya, anomaliyalarni aniqlash, Big data

Аннотация: В данной работе проводится сравнительный анализ алгоритмов электронной цифровой подписи DSA и ECDSA с точки зрения их математических основ, принципов функционирования и практического применения. Рассматриваются сходства и различия алгоритмов, их криптографическая стойкость, длина ключей и вычислительная эффективность. Особое внимание уделяется уязвимости алгоритма ECDSA, связанной с повторным использованием случайного параметра k , что может привести к раскрытию закрытого ключа.

Кроме того, в статье исследуются возможности применения методов искусственного интеллекта и машинного обучения для анализа электронных цифровых подписей. Показано, что использование методов классификации, кластеризации и обнаружения аномалий позволяет выявлять скрытые зависимости, статистические отклонения и потенциальные угрозы в больших массивах данных.

Ключевые слова: DSA, ECDSA, электронная цифровая подпись, искусственный интеллект, машинное обучение, криптография, обнаружение аномалий, Big data

Annotation: This paper presents a comparative analysis of DSA and ECDSA digital signature algorithms, focusing on their mathematical foundations, operational principles, and key differences. The algorithms are evaluated in terms of cryptographic strength, key size, and computational efficiency. Special attention is given to the security vulnerability of ECDSA related to the reuse of the random parameter k , which may lead to private key disclosure.

In addition, the paper explores the application of artificial intelligence and machine learning techniques for analyzing digital signatures. It demonstrates how classification, clustering, and anomaly detection methods can be used to identify hidden vulnerabilities and abnormal patterns within large-scale cryptographic data.

Key words: DSA, ECDSA, digital signature, machine learning, cryptography, anomaly detection, Big data

Hozirgi kunda jamiyatning tez sur'atlarda raqamlashtirilishi elektron hujjatlar, onlayn to'lovlar, taqsimlangan tizimlar hamda bulutli texnologiyalar xavfsizligini ta'minlashni muhim masalaga aylantirdi. Elektron raqamli imzo (ERI) esa axborotning haqiqiylikni tasdiqlash, uning

yaxlitligini saqlash va muallif tomonidan inkor etilmasligini kafolatlashda asosiy vositalardan biri hisoblanadi[1].

Raqamli iqtisodiyotning rivojlanishi natijasida yaratilayotgan va tekshirilayotgan elektron imzolar soni keskin oshmoqda. Bu holat kriptografik algoritmlarni nafaqat matematik jihatdan, balki katta hajmdagi ma'lumotlarni intellektual tahlil qilish orqali ham o'rganishni talab etmoqda. Shu bilan birga, sun'iy intellekt texnologiyalari ham kiberxavfsizlik sohasida keng qo'llanila boshladi.

Natijada, elektron raqamli imzo algoritmlarining ishonchliligini baholash va ularning zaif tomonlarini aniqlash uchun an'anaviy kriptografiya usullarini mashinaviy o'qitish texnologiyalari bilan uyg'unlashtirish dolzarb vazifalardan biriga aylandi.

Elektron raqamli imzo matematik jihatdan bir nechta algoritmlar to'plami orqali ifodalanadi[1]:

$$(G, S, V)$$

Bu yerda:

G- kalit yaratish algoritmi : $G \rightarrow (e, d)$ (e- ochiq kalit, d- maxfiy kalit)

S- imzo yaratish algoritmi: $S(d, m) \rightarrow k$ (m-xabar, k-elektron imzo)

V- imzoni tekshirish algoritmi: $V(e, m, k) \rightarrow \{0, 1\}$ (1-haqiqiy imzo, 0- noto'g'ri imzo)

Tizimning to'g'ri ishlashi quyidagi shart orqali aniqlanadi:

$$V(e, m, S(d, m)) = 1$$

Bu shuni bildiradiki, maxfiy kalit yordamida yaratilgan imzo ochiq kalit orqali muvaffaqiyatli tekshirildi.

Elektron raqamli imzoning xavfsizligi maxfiy kalitni bilmagan holda imzoni qalbakilashtirib bo'lmazligiga asoslanadi.

DSA (Digital Signature Algorithm)-diskret logarifmlash masalasiga asoslangan elektron raqamli imzo algoritmi hisoblanadi[4].

Kalit yaratish:

$$y = g^x \mod p$$

- p- tub son
- g- generator
- x- maxfiy kalit
- y- ochiq kalit

Imzo yaratish:

$$r = (g^k \mod p) \mod q, s = k^{-1}(h(m) + xr) \mod q$$

- m- yuborilayotgan xabar
- h(m)- xabarning xesh qiymati
- k- tasodofiy son
- r, s- imzo

Imzoni tekshirish:

$$v = (g^{u_1} y^{u_2} \mod p) \mod q$$

$$[u_1 = h(m)w \mod q; u_2 = rw \mod q; w = s^{-1} \mod q]$$

Agar $v=r$ bo'lsa, imzo haqiqiy hisoblanadi.

ECDSA (Elliptic Curve Digital Signature Algorithm)-elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmi hisoblanadi[3].

Elliptik egri chiziq tenglamasi:

$$y^2 = x^3 + ax + b \bmod p$$

- a,b- egri chiziqli parametrlari
- p- katta tub son
- x,y- egri chiziqli nuqtalari

Kalit yaratish:

$$Q = dG$$

- d- maxfiy kalit
- G- bazaviy nuqta
- Q- ochiq kalit

Imzoni yaratish:

$$R = kG$$

$$r = x_R \bmod ns = k^{-1}(h(m) + dr) \bmod n$$

- m- xabar
- h(m)- xabar xeshi
- k- tasodifiy son
- r,s- elektron imzo
- n- elliptik egri chiziqli bazaviy nuqta G ning tartibi

Imzoni tekshirish:

$$Ch = u_1G + u_2Qr = x_{Ch} \bmod n [u_1 = h(m)w \bmod n; u_2 = rw \bmod n; w = s^{-1} \bmod n]$$

Agar r qiymati imzodagi r bilan teng bo'lsa, imzo haqiqiy hisoblanadi.

ECDSA algoritmi kichik kalit o'lchamlarida ham yuqori kriptobardoshlilikni ta'minlay oladi va bu bilan DSA dan sezilarli darajada farq qiladi, chunki DSA da xavfsizlikni saqlab qolish uchun katta kalit o'lchamlarini talab qiladi.

Lekin, ECDSA algoritmi barcha holatlarda ham mulaqo xavfsiz emas. Agar imzo yaratishda bir xil k qiymati takroran ishlatilsa, bu yopiq kalitning ochilishiga olib keladi[5].

Misol uchun: m_1 va m_2 berilgan.

Ularning xeshlari:

$$xesh_1 = h(m_1) \quad xesh_2 = h(m_2)$$

Imzolari:

$$(r, s_1)(r, s_2)$$

Bu yerdan:

$$s_1 = k^{-1}(h_1 + dr)$$

$$s_2 = k^{-1}(h_2 + dr)$$

Ularni ayirib:

$$s_1 - s_2 = k^{-1}(h_1 - h_2)$$

Natijada k quyidagicha topiladi:

$$k = (h_1 - h_2)(s_1 - s_2)^{-1} \bmod n$$

Keyingi bosqichda yopiq kalit aniqlanadi:

$$d = (s_1k - h_1)r^{-1} \bmod n$$

Shunday qilib, tasodifiy parametrlarning takrorlanishi yopiq kalitning ochilishiga olib keladi.

DSA va ECDSA algoritmlari turli matematik asosga ega bo'lishiga qaramay, ularning imzo yaratish mexanizmi o'xshash strukturaga ega. Har ikkala algoritm ham quyidagi imzo tuzilmasidan foydalanadi:

$$s = k^{-1}(h(m) + dr)$$

Lekin, matematik asoslari(DSA- modul arifmetika, ECDSA- elliptik egri chiziqlar), kalit uzunligi va xavfsizlik darajasi o'rtasidagi nisbat, hisoblash samaradorligi jihatlari tomonidan farqlanadi.

Yuqorida ko'rib chiqilgan ikki algoritm matematik jihatdan yuqori kriptobardoshlikni ta'minlasada, ularning xavfsizligi nafaqat nazariy asosga, balki amaliy realizatsiyaga ham bog'liq. Amaliy tizimlarda yuzaga keladigan tasodifiy parametr k ning noto'g'ri generatsiyasi, zaif kalitlar yoki noto'g'ri konfiguratsiya kabi xatoliklar an'anaviy matematik tahlil orqali har doim ham aniqlanmasligi mumkin. Shu sababli, zamonaviy kriptografik tizimlarni tahlil qilishda suniy intellekt va mashinaviy o'rganish usullaridan foydalanish dolzarb yo'nalishlardan biriga aylanmoqda.

Sun'iy intellekt va mashinaviy o'rganish katta hajmdagi ma'lumotlarni avtomatik ravishda tahlil qilish, yashirin bog'lanishlarni aniqlash va murakkab tizimlarda anomaliyalarni aniqlash imkonini beradi[6]. Kriptografik tizimlarda bu yondashuv asosan algoritmlarni buzish uchun emas, balki uning amalga oshirishda zaifliklarini aniqlash uchun qo'llaniladi[6].

ERI ni AI yordamida tahlil qilishda imzo quyidagi belgilar to'plami sifatida qaraylik:

$$X = (r, s, h(m), v, kID, qID)$$

- r, s - imzo parametrlari
- $h(m)$ - xabar xeshi
- v - vaqt
- kID -kalit identifikatori
- qID - qurilma identifikatori

Mazkur yondashuv kriptografik obyektni statistik va ehtimollik nuqtai nazaridan tahlil qilish imkonini beradi.

Mashinaviy o'rganishda klassifikatsiya usulidan foydalanilganda, u elektron raqamli imzolarni oldindan belgilangan sinflarga ajratish imkonini beradi. Ushbu yondashuv mavjud ma'lumotlar asosida modelni o'rgatish va yangi imzolarni baholashga xizmat qiladi.

Natijada klassifikatsiya usuli quyidagi asosiy vazifalarni bajaradi:

- Imzolarni normal va shubhali guruhlariga ajratish
- Zaif kalitlar bilan yaratilgan imzolarni aniqlash
- Noto'g'ri ishlov berilgan imzolarni topish

Matematik ko'rinishi:

$$P(y|X)$$

- X -imzo belgilari vektori
- y -sinf(normal va shubhali)

Mazkur model kiruvchi imzo parametrlariga asoslanib, uning qaysi sinfga tegishli ekanligini ehtimollik nuqtai nazardan baholaydi.

Klassifikatsiyadan farqli ravishda, klasterlash nazoratsiz o'rganish usuliga kiradi. Bu usulda ma'lumotlar oldindan belgilangan sinflarga ega bo'lmaydi va algoritm imzolar orasidagi o'xshashlik darajasiga qarab ularni mustaqil ravishda guruhlariga ajratadi.

Elektron raqamli imzolarni tahlil qilishda klasterlash quyidagi vazifalarni bajaradi:

- o'xshash parametrli imzolarni bir guruhga jamlash
- tizim ichidagi yashirin struktura va qonuniyatlarni aniqlash
- noodatiy imzolarni aniqlash
- turli foydalanuvchi yoki qurilmalar bilan bog'liq imzolarni ajratish

Klasterlashning eng keng tarqalgan algoritmlaridan biri K- means hisoblanadi. Ushbu algoritim ma'lumotlarni k ta klasterga ajratadi va quyidagi maqsad funksiyasini minimallashtiradi:

$$\sum_{i=1}^k \sum_{x \in C_i} \|x - \mu_i\|^2$$

- C_i – i-chi klaster
- μ_i - klaster markazi
- x - imzo belgilari vektori

Mazkur yondashuv orqali tizimdagi ko'p sonli imzolar ichidan o'ziga xos xususiyatlarga ega guruhlarini ajratish mumkin. Agar ayrim imzolar hech bir klasterga yaqin bo'lmasa yoki alohida kichik guruh hosil qilsa, ular potensial xavfli yoki shubhali sifatida baholanishi mumkin.

Elektron raqamli imzolar xavfsizligini ta'minlashda eng muhim yo'nalishlardan biri - bu anomaliyalarni aniqlashdir. Anomaliya - bu tizimdagi odatiy xatti-harakatlardan keskin farq qiluvchi holatdir.

Kriptografik tizimlarda bunday holatlar ko'pincha quyidagi sabablar bilan bog'liq bo'ladi:

- tasodifiy parametr k ning takrorlanishi
- zaif yoki noto'g'ri ishlayotgan tasodifiy son generatori
- kalitlarning noto'g'ri ishlatilishi
- tashqi hujumlar yoki komprometatsiya

Masalan, agar ECDSA algoritmidagi quyidagi holat kuzatilsa[5]:

$$r_1 = r_2$$

bu ikki xil xabar uchun bir xil k ishlatilganini bildiradi va bu yopiq kalitning ochilishiga olib kelishi mumkin.

Xulosa qilib aytganda, DSA va ECDSA algoritmlari elektron raqamli imzo tizimlarida muhim ahamiyatga ega bo'lib, ularning xavfsizligi murakkab matematik masalalarga tayanadi. Olib borilgan tahlillar shuni ko'rsatadiki, ECDSA algoritmi kichik kalit uzunligida ham yuqori darajadagi xavfsizlikni ta'minlay oladi va shu sababli zamonaviy axborot tizimlarida keng qo'llanilmoqda.

Biroq, ushbu algoritmlarning ishonchliligi faqat nazariy jihatlariga emas, balki ularning amalda qanday qo'llanilishiga ham bevosita bog'liq. Ayniqsa, tasodifiy parametr k noto'g'ri generatsiya qilinsa yoki takroran ishlatilsa, bu yopiq kalitning ochilishiga olib kelishi mumkin. Bu esa butun tizim xavfsizligi uchun jiddiy xavf tug'diradi.

Tadqiqot davomida mashinaviy o'rganish usullaridan foydalanish elektron raqamli imzolarni tahlil qilishda samarali yondashuv ekanligi aniqlandi. Klassifikatsiya, klasterlash va anomaliyalarni aniqlash kabi usullar yordamida katta hajmdagi ma'lumotlar ichidan yashirin zaifliklarni, noodatiy holatlarni hamda potensial xavfli vaziyatlarni aniqlash mumkin.

Kelajakda sun'iy intellekt texnologiyalari kriptografik tizimlarning muhim tarkibiy qismiga aylanishi kutilmoqda. Ular real vaqt rejimida monitoring olib borish, xavflarni oldindan aniqlash va tizimlarni avtomatik tahlil qilish imkonini beradi. Shu bilan birga, AI texnologiyalarining rivojlanishi yangi turdagi tahdidlarni ham yuzaga keltirishi mumkin. Bu esa kriptografiya va sun'iy intellekt o'rtasida muvozanatni saqlash qanchalik muhim ekanligini yana bir bor ko'rsatadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. National Institute of Standards and Technology. (2023). Digital Signature Standard (FIPS 186-5). NIST, 1-35, 43-65 b.
2. Barker, E. (2020). Recommendation for Key Management (SP 800-57). NIST, 50-70 b.

- 
3. Johnson, D., Menezes, A., Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm. IJIS, 1-13 b.
 4. Menezes, A.(1996).Handbook of Applied Cryptography.CRC Press, 400-470b.
 5. Pornin, T. (2013). RFC 6979: Deterministic Usage of the Digital Signature Algorithm (DSA and ECDSA). IETF, 1-25 b.
 6. ENISA. (2024). Threat Landscape 2024. EU, 10-75 b.
 7. Kak, A. (2025). Computer and Network Security. Purdue University, 9-18,22-30, 44-57 b.