POLINOMIAL HESH FUNKSIYALAR ASOSIDA MA'LUMOT XAVFSIZLIGINI TA'MINLASH

Jumaniyozov Firuz
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti, Axborot xavfsizligi kafedrasi o'qituvchisi

Qabul qilindi: 16.10.2025
Ko'rib chiqildi: 17.10.2025
Tasdiqlandi: 18.10.2025

Kalit so'zlar: polinomial hesh, kriptografiya, ma'lumot xavfsizligi, integritet, lavina effekti, autentifikatsiya, raqamli imzo.

Annotatsiya. Ushbu maqolada axborot xavfsizligini ta'minlashda polinomial hesh funksiyalarining nazariy asoslari va ularning qo'llanilish imkoniyatlari yoritilgan. Polinomial hesh funksiyalar ma'lumotlarning yaxlitligini nazorat qilish, autentifikatsiya va raqamli imzo tizimlarida ishonchli mexanizm sifatida ishlatilishi ko'rsatib o'tilgan. Tadqiqotda hesh funksiyalarining asosiy xususiyatlari, xususan to'qnashuvga qarshilik, lavina effekti va bir yo'naliklilik talablari tahlil qilinadi. Shuningdek, polinomial heshning samaradorligi va kriptografik barqarorligi haqida amaliy tahlillar keltiriladi.

Kirish. Axborot xavfsizligi sohasida ma'lumotlarning yaxlitligini ta'minlash muhim ahamiyatga ega. Ma'lumotlar uzatilish yoki saqlanish jarayonida o'zgarishi, buzilishi yoki soxtalashtirilishi mumkin. Shu bois, bunday holatlarni aniqlash va oldini olishda hesh funksiyalardan keng foydalaniladi. Hesh funksiya kirish ma'lumotidan o'lchami qat'iy belgilangan raqamli qiymat (hesh) hosil qiladi. Bu qiymat orqali ma'lumot o'zgarganligini tezda aniqlash mumkin. Ayniqsa, polinomial hesh algoritmlari o'zining soddaligi va samaradorligi bilan ajralib turadi.

Polinomial hesh funksiyasi mohiyati

Polinomial hesh funksiyasi odatda quyidagi matematik ifoda bilan ta'riflanadi:

$$H(s) = (s_1 \cdot p^{(k-1)} + s_2 \cdot p^{(k-2)} + \ldots + s_k) \bmod m$$

Bu yerda:
s_i — ma'lumotning i-elementi (masalan, belgining ASCII kodi),
p — tanlangan asos (odatda tub son, masalan 31 yoki 53),
m — modul (odatda katta tub son, xesh to'qnashuvlarini kamaytiradi).
Mazkur modelning asosiy afzalligi shundaki, u **tez hisoblanadi, kolliziyaga chidamli**, va **xotira jihatidan samarali.** Polinomial hesh algoritmi ko'pincha **Rolling Hash** (sliding window hashing) usuli bilan birgalikda qo'llaniladi, bu esa ma'lumot oqimini tahlil qilishda (masalan, virus skanerlash, fayl solishtirish yoki raqamli imzo tizimlarida) yuqori samaradorlik berad

Polinomial hesh algoritmlari matnli ma'lumotlarni, xabarlar ketma-ketligini va fayllarni tez va ishonchli tarzda heshga aylantirish imkonini beradi. Bu usul, xususan, string matching, blokcheyn va raqamli imzo tizimlarida samarali qo'llaniladi.

Xususiyatlari va afzalliklari

1. Bir yo'naliklilik – Heshdan asl ma'lumotni qayta tiklash amalda imkonsiz.
2. To'qnashuv qarshiligi – Turli ma'lumotlar uchun bir xil hesh hosil bo'lish ehtimoli juda past.
3. Lavina effekti – Ma'lumotdagi bitta belgining o'zgarishi butun hesh qiymatini sezilarli o'zgartiradi.
4. Soddalik va tezlik – Polinomial heshlar murakkab matematik operatsiyalarni talab qilmaydi, bu esa ularni resurs cheklangan tizimlarda ishlatishga imkon beradi.

Qo'llanilish sohalari

• Parollarni himoyalash – foydalanuvchi parolini saqlashda faqat uning hesh qiymati bazaga yoziladi.
• Raqamli imzolar – ma'lumotlar yaxlitligini tekshirishda hesh qiymati imzo bilan birgalikda ishlatiladi.
• Blokcheyn tizimlari – har bir blokning hesh qiymati oldingi blok bilan bog'lanadi.
• Fayl yaxlitligini nazorat qilish – tizimdagi o'zgarishlarni aniqlashda hesh solishtirish usuli qo'llaniladi.

Tadqiqotlar shuni ko'rsatadiki, polinomial hesh algoritmi kichik hajmli matnlar va real vaqt tizimlari uchun yuqori samaradorlikka ega. Ammo kriptografik darajada mustahkam xavfsizlik talab etiladigan tizimlarda (masalan, moliyaviy operatsiyalar) SHA-3 yoki BLAKE2 kabi algoritmlar bilan birgalikda qo'llanishi tavsiya etiladi

Xulosa. Polinomial hesh funksiyalar soddaligi, tezligi va samaradorligi bilan ajralib turadi hamda ma'lumotlarning yaxlitligini ta'minlashda muhim vosita hisoblanadi. Ular kichik va o'rta miqyosli tizimlarda samarali ishlaydi, parollarni himoyalash, ma'lumotlarni autentifikatsiya qilish va blokcheyn mexanizmlarida asosiy komponentlardan biri sifatida qo'llanilishi mumkin.

Shuningdek, polinomial heshlar o'zining matematik moslashuvchanligi tufayli turli modul va asos sonlari orqali optimallashtirilishi mumkin. Bu esa ularni tizim arxitekturasi, ma'lumot hajmi va xavfsizlik darajasiga moslashtirish imkonini beradi. Kelgusida bu algoritmlarni kvant xavfsiz kriptotizimlar bilan integratsiyalash, GPU asosida tezlashtirish hamda chuqur o'rganish (deep learning) modellarida xesh sifatida ishlatish istiqbollari mavjud. Natijada, polinomial hesh funksiyalar zamonaviy axborot xavfsizligi infratuzilmasining engil, lekin ishonchli komponenti sifatida dolzarbligini saqlab qoladi.

Foydalanilgan adabiyotlar

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1996.
2. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.
3. Schneier B. Applied Cryptography. Wiley, 2015.
4. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978.
5. National Institute of Standards and Technology (NIST). FIPS PUB 180-4: Secure Hash Standard (SHS), 2015.
6. Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997.
7. Wang X., Yu H. How to Break MD5 and Other Hash Functions. Advances in Cryptology – EUROCRYPT, 2005.
8. Babenko M.A., Khashin S.A. Polynomial Rolling Hash Function for Text Comparison. Journal of Computer Science, 2021.
9. Rogaway P., Shrimpton T. Cryptographic Hash-Function Basics. Fast Software Encryption, 2004.
10. https://en.wikipedia.org/wiki/Polynomial_hash_function