MIRZO ULUG'BEK NOMIDAGI
O'ZBEKISTON MILLIY UNIVERSITETINING
JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

RESPUBLIKA ILMIY-TEXNIK ANJUMAN MATERIALLARI TO‘PLAMI

15-16-MAY
2026-YIL

doi

Google Scholar

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami

(2026-yil 15-16-may)

JIZZAX-2026

8. Qin L., Hsu J., Stern M. Evaluating the usage of cloud-based collaboration services through teamwork. Journal of Education for Business, 2016, 91(4), pp. 227-235.
9. Aaron L. S., Roche C. M. Teaching, Learning, and Collaborating in the Cloud: Applications of Cloud Computing for Educators in Post-Secondary Institutions. Educational Technology, 2012, 40(2), pp. 95-111.
10. Dogan M. E., Dogan T. G., Bozkurt A. The Use of Artificial Intelligence in Online Learning and Distance Education Processes: A Systematic Review of Empirical Studies. Applied Sciences, 2023, 13(5), 3056.

KRIPTOGRAFIK ALGORITMLAR VA HISOBLASH MURAKKABLIGI: IT TARMOQLARI XAVFSIZLIGINI TA`MINLASHGA MATEMATIK YONDASHUV

Yusupov Behzod Ismoil o`g`li

begzody231@gmail.com

Nomozboyeva Parizod G`ayrat qizi

parizodnomozboyeva@gmail.com

Eshquvvatova Hulkar G`ulomjon qizi

hulkareshquvvatova4@gmail.com

Abdurazzoqova Dilnura Komiljon qizi

abdurazzoqovadilnura06@gmail.com

O’zbekiston Milliy universiteti Jizzax filiali

Annotatsiya: Kriptografik algoritmlar ma'lumotlar maxfiyligi, yaxlitligi va autentifikatsiyasi orqali IT tarmog'ini himoya qilishning markazida turadi. Ushbu tadqiqot to'rtta kriptografik algoritmning hisoblash samaradorligi va murakkabligini o'rganadi: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Panjara asosidagi kriptografiya (LBC) va Giperelliptik egri chiziqli kriptografiya (HECC). Tadqiqot ushbu algoritmlarni shifrlash vaqti, shifrni ochish vaqti, kalit yaratish vaqti va xavfsizlik kuchidan foydalangan holda taqqoslaydi. Tajriba natijasi shuni ko'rsatadiki, AES real vaqt rejimida qo'llanilishi uchun optimal shifrlash vaqtiga 2,3 ms va RSA maksimal shifrlash vaqtiga 15,7 ms ni tashkil etadi, bu esa hisoblash xarajatlarini ta'kidlaydi. Kvantdan keyingi istiqbolli kriptografik usul bo'lgan LBC o'rtacha 8,9 ms shifrlash vaqti bilan kuchli xavfsizlikni ta'minlaydi, HECC esa 5,4 ms shifrlash vaqti bilan xavfsizlik va samaradorlik o'rtasidagi muvozanatni ta'minlaydi. Qiyosiy tahlil shuni ko'rsatadiki, panjara asosidagi shifrlash kelajakda kvantga chidamli xavfsizlikdan foydalanish uchun eng mos keladi va AES yuqori tezlikdagi shifrlash uchun eng yaxshi qo'llaniladi. Tadqiqot xavfsizlik ehtiyojlari va hisoblash samaradorligiga muvofiq to'g'ri kriptografik algoritmlarni tanlash zarurligini ta'kidlaydi. Kelajakdagi tadqiqotlar, shuningdek, kelajakdagi IT infratuzilmasida

xavfsizlikni yaxshilash uchun gibrid kriptografik modellar va AI asosidagi shifrlash usullariga qaratilishi kerak.

Kalit so'zlar: Kriptografik algoritmlar, Hisoblash murakkabligi, Post-kvant Kriptografiya, IT xavfsizligi, shifrlash samaradorligi.

Raqamli aloqa va almashinuvga tobora ortib borayotgan qaramlik bilan axborot-kommunikatsiya texnologiyalari tarmoqlari endi muhim ahamiyat kasb etmoqda. Kriptografik algoritmlar maxfiylik, yaxlitlik va haqiqiylikka ta'sir qiluvchi maxfiy ma'lumotlarni himoya qilish uchun javobgardir. Shunga qaramay, kriptografik xavfsizlikning samaradorligi ushbu algoritmlarning hisoblash murakkabligiga bog'liq, chunki ular o'zlarini hujumlarga chidamli va bunday dasturlarda amalda qo'llanilishi mumkin . Ushbu tadqiqot kriptografik algoritmlarning asoslarini matematik nuqtai nazardan o'rganadi va ularning IT tarmog'idagi xavfsizligi va samaradorligini baholaydi. Zamonaviy kriptografik tizimlarda qo'llaniladigan ko'plab tamoyillar sonlar nazariyasi, algebraik tuzilmalar va murakkablik nazariyasi g'oyalarini o'z ichiga oladi. Masalan, RSA, Elliptik egri chiziqli kriptografiya (ECC) va panjara asosidagi shifrlash kabi ochiq kalitli kriptografiyaga asoslangan muammolar hisoblash jihatidan qiyin deb hisoblanadi, masalan, butun sonli faktorizatsiya va diskret logarifmlar . Xuddi shu narsa AES va simmetrik kalitli kriptografiya ChaCha20, kriptoanaliz qilib bo'lmaydigan juda murakkab transformatsiyalarga tayanadi. Kvant hisoblashlari yaxshilanishi bilan raqiblar o'zlarining hisoblash quvvatini oshirishlari mumkin, shuning uchun bu algoritmlarni qiyinlashtiradigan taxminlarni chuqurroq tushunish zarur bo'ladi . Ushbu tadqiqot turli kriptografiya algoritmlari hisoblash samaradorligi va xavfsizlik o'rtasida qanday qilib oqilona muvozanatga erishganligini o'rganadi. Tadqiqot shuningdek, tobora ortib borayotgan kibertahdidlarga qarshi kurashishda yordam berish uchun post-kvant kriptografiyasi va gomomorfik shifrlash kabi yangi paydo bo'layotgan kriptografik paradigmalarni ham o'rganadi. Bundan tashqari, tadqiqot hisoblash murakkabligi sinflaridan (P, NP, NP-hard, NP) foydalanish bilan bog'liq kriptografik tizimlarning xavfsizlik kafolatlarini ko'rib chiqadi.

1. Bulutli xavfsizlik uchun kriptografik yechimlar

Xavfsizlik bulutli hisoblash uchun ma'lumotlar maxfiyligi va maxfiyligi borasidagi asosiy muammolardan biridir. Dawson va boshqalar tomonidan bulutli muhit uchun taklif qilingan kriptografik yechimlar o'zlarining ishlash vaqtida turlicha tendentsiyalarni namoyon etishi ko'rsatilgan. Ularning tadqiqotining asosiy diqqatga sazovor jihati shundaki, Advanced Encryption Standard (AES) xavfsizlik va hisoblash samaradorligi o'rtasida yaxshi muvozanatni ta'minlaydi, shuning uchun bulutga asoslangan shifrlashda afzalroqdir. Shunga qaramay, mualliflar RSA (assimetrik shifrlash) yuqori darajadagi hisoblash xarajatlarini talab qilishini va shu bilan real vaqt rejimida bulutli ilovalar uchun mos kelmasligini ham ta'kidladilar.

2. Kriptografiyada hisoblash muammolari

Kriptografik tizimlarda kalitlarni yaratish va hisoblash samaradorligi asosiy masalalardan biri sifatida qaraladi. RSA va boshqa assimetrik shifrlash sxemalarida tub sonlarni yaratish juda muhim ahamiyat kasb etadi. Va ular o'z tadqiqotlarida tub

sonlarni yaratish jarayonini tezlashtirish uchun yangi algoritmlarni ishlab chiqdilar, bu esa natijada yuqori darajadagi xavfsizlikni saqlab qolish bilan birga kalitlarni yaratish uchun zarur bo'lgan vaqtni qisqartiradi.

3. Kvantdan keyingi kriptografiya va kelajakdagi yo'nalishlar

Post-kvant kriptografiyasini rivojlantirishga qaratilgan sa'y-harakatlarning barchasi kvant kompyuterlari keltirib chiqaradigan potentsial tahdidlar tufayli juda yaxshi. Post-kvant kriptografik texnikalarni va klassik shifrlashdan kvantga chidamli algoritmlarga o'tishdagi qiyinchiliklarni keng qamrovli ko'rib chiqishda Kanza va boshqalar ushbu muammolarning barchasini ko'rib chiqdilar. Ular kvantdan keyingi xavfsizlikni ta'minlashda panjara asosidagi kriptografiya va xesh asosidagi kriptografiya istiqbolli nomzodlar ekanligini aniqladilar.

4. Yangi kriptografik usullar va qo'llanmalar

Turli sohalarda xavfsizlikni oshirish uchun boshqa kriptografik yechimlar ham qo'llanilmoqda. Marius Alin Dragu va boshqalar miya to'lqini naqshidan olingan kriptografik algoritm yaratdilar. Ushbu yondashuv asosan shifrlash kalitlarini yaratish uchun biometrik signallarning orqa tomoniga yangi xavfsizlik qatlamini qo'shdi. Ular natijalari standart kriptografik usullarga qaraganda tasodifiylik va xavfsizlikni oshirganligini aniqladilar.

Kengaytirilgan shifrlash standarti (AES) - Simmetrik shifrlash

AES - bu ma'lumotlarni 128 bitli bloklarga uzatish va mos keladigan shifrni ochish uchun ishlatiladigan blok shifr. Yuqori xavfsizlik va hisoblash samaradorligi uchun u 128, 192 yoki 256 bitli kalit uzunligiga ega . Shifrlash jarayoni bir necha bosqichli almashtirish, permutatsiya, aralashtirish va kalit qo'shishni o'z ichiga oladi.

RSA - Asimmetrik shifrlash

AES - bu ma'lumotlarni 128 bitli bloklarga uzatish va mos keladigan shifrni ochish uchun ishlatiladigan blok shifr. Yuqori xavfsizlik va hisoblash samaradorligi uchun u 128, 192 yoki 256 bitli kalit uzunligiga ega . Shifrlash jarayoni bir necha bosqichli almashtirish, permutatsiya, aralashtirish va kalit qo'shishni o'z ichiga oladi.

RSA butun sonlarni faktorizatsiyalashning murakkabligiga asoslangan ochiq kalitli kriptotizimdir. U xavfsiz kalit almashinuvi va raqamli imzolar uchun keng qo'llaniladi

Elliptik egri chiziqli kriptografiya (ECC) – Asimmetrik shifrlash

ECC - bu RSA bilan bir xil darajadagi xavfsizlikni ta'minlaydigan, ammo ancha kichikroq kalit o'lchamlariga ega bo'lgan ochiq kalitli kriptosistema. U elliptik egri chiziqning qattiqligi asosida diskret logarifm muammosi (ECDLP) asosida yaratilgan.

SHA-256 – Kriptografik xesh funksiyasi

SHA-256 - bu har qanday kirish uchun o'zgarmas 256-bitli chiqishni yaratadigan kriptografik xesh funksiyasi. U ma'lumotlar yaxlitligini va blokcheyn xavfsizligini tekshirish uchun keng qo'llaniladi

Ushbu tadqiqotning asosiy maqsadi kriptografik algoritmlarning matematik va hisoblash jihatlariga va ularni IT tarmoqlarini himoya qilishda qanday qo'llash

mumkinligiga qaratildi. Kiberxavfsizlik raqamli landshaft bir-biriga ko'proq bog'langanligi sababli ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini himoya qilishda muhim ahamiyatga ega bo'lgan kriptografiyani o'z ichiga oladi. Ushbu tadqiqotda bir nechta kriptografik yechimlar tahlil qilindi va turli xil simmetrik shifrlash, assimetrik shifrlash, postkvant kriptografiyasi va yengil kriptografik texnikalarning afzalliklari va kamchiliklari aniqlandi. Kriptografik algoritmlarni taqqoslash orqali biz Advanced Encryption Standard (AES) xavfsizlik va samaradorlik jihatidan muvozanati tufayli keng qo'llanilishini, Rivest-Shamir-Adleman (RSA) esa hisoblash xarajatlarida yaxshi ustunlikni saqlab qolganini ko'ramiz. Tadqiqot tomonidan yangi paydo bo'layotgan kriptografik tendentsiyalar ham o'rganildi - xususan, panjara shifrlash va giperelliptik egri chiziq postkvant xavfsizlikka istiqbolli alternativa bo'lgan kriptografiyaga ega edi.

Foydalanilgan adabiyotlar:

1.ABIDEMI, EA, MISRA, S., ENIOLA, D. va BOKOLOJR, A., 2022. O'zgartirilgan hisoblash murakkabligi Blowfish video ma'lumotlaridagi kriptografik algoritm. Algoritmlar, 15(10), 373-betlar.

2. ADENIYI, AE, ABIODUN, KM, AWOTUNDE, JB, OLAGUNJU, M., OJO, OS va EDET, NP, 2023 yil. Bulutli muhitda tibbiy axborot xavfsizligi uchun blok shifrlash algoritmini joriy etish: o'zgartirilgan ilg'or shifrlash standart yondashuvidan

foydalanish. Multimedia vositalari va ilovalari, 82(13), 20537-betlar

3. AGA, DT, CHINTANIPPU, R., MOWRI, RA va SIDDULA, M., 2024. Narsalar interneti uchun xavfsiz va maxfiy ma'lumotlarni yig'ish usullarini o'rganish: keng qamrovli sharh. Narsalar internetini kashf eting, 4(1), 28-betlar.

4.AHMED ABD, AA, ALI, SM va MOHANAD, RG, 2024. Modifikatsiyalangan XTEA yordamida ma'lumotlarni shifrlash bloki

Algoritm. Axborot tizimlari muhandisligi, 29(3), 1075-1083-betlar.

5.AKIMOVA, O., ZHYDOVSKA, N., KUCHMIIOVA, T., KOZITSKA, N. va BURYAK, I., 2024. Buxgalteriya hisobida moliyaviy ma'lumotlarni kiberhimoya qilish: Kriptografik usullarni joriy etish va ulardan foydalanish. Iqtisodiy ishlar, 69(2), 1041-1052-betlar

AXBOROT TIZIMLARINI YARATISH TEXNOLOGIYALARI VA FREYMVORKLARI

Olimova Muxlisa Vohidjon qizi
Toshkent davlat iqtisodiyot universiteti
Sun’iy intellekt kafedrasi katta o‘qituvchisi
mukhlis.olimova1323@gmail.com

Abdumalikov Akmaljon Abduxoliq o‘g‘li

t.f.f.d., PhD., Dotsent. O‘zMU Jizzax filiali

Ilmiy tadqiqotlar, innovatsiyalar va ilmiy

pedagog kadrlarni tayyorlash bo‘limi boshlig‘i