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

10. Evans, D., Song, J. Raqamli iqtisodiyot va logistika kelajagi. – Jahon iqtisodiy forumi (WEF) hisoboti, 2023.

GOMOMORF SHIFRLASH ASOSIDA BULUTLI SAQLASH TIZIMLARIDA MA'LUMOTLAR MAXFIYLIGINI TA'MINLASH USULLARI.

Yusupov Bekzod

behzody231@gmail.com

Po'latova Feruza

fpolatova908@gmail.com

Mamadiyorova Gulsevar

Mirzo Ulug'bek nomidagi O'zbekiston

Milliy universiteti Jizzax filiali

Axborot tizimlari va texnologiyalari talabasi

Annotatsiya. Ushbu maqolada ishonchsiz bulutli muhitda ma'lumotlar maxfiyligini saqlash muammosi va uni hal etishda To'liq Gomomorfik Shifrlash (FHE) texnologiyasining qo'llanilishi tadqiq qilingan. Paillier, BFV va CKKS kriptografik sxemalarining matematik asoslari hamda unumdorlikka ta'siri qiyosiy tahlil qilindi. Shuningdek, LWE va panjara nazariyasiga asoslangan algoritmlarning kvant kompyuterlariga chidamliligi ko'rib chiqildi. Natijalar FHE yuqori xavfsizlikni ta'minlashini, biroq hisoblash xarajatlarini sezilarli oshirishini ko'rsatdi.

Abstract. This article explores the problem of data privacy in an unreliable cloud environment and the application of fully homomorphic encryption (FHE) technology in its solution. A comparative analysis was made of the mathematical foundations of the cryptographic schemes of Paillier, BFV and CKKS, as well as the effect on productivity.

Kalit so'zlar:Gomomorfik shifrlash, FHE, Ma'lumotlar bazasi xavfsizligi, Bulutli hisoblash, Paillier kriptotizimi, Bootstrapping, Panjara (Lattice) nazariyasi, LWE, Post-kvant kriptografiya.

Keywords: Homomorphic encryption, FHE, Database security, Cloud computing, Paillier cryptosystem, Bootstrapping, Noise, Lattice theory, LWE, Post-quantum cryptography.

Jahon iqtisodiyoti va davlat boshqaruvida raqamli transformatsiya jarayonlari bulutli hisoblash platformalaridan keng foydalanishga olib keldi. AWS, Google Cloud va Microsoft Azure kabi tizimlar iqtisodiy samaradorlik va masshtablash imkonini

bersa-da, ma’lumotlar maxfiyligi va suvereniteti bilan bog‘liq xavflarni yuzaga chiqarmoqda.An’anaviy axborot xavfsizligi ma’lumotlarni saqlash va uzatishda samarali himoya qilsa ham, qayta ishlash jarayonida ma’lumotlarni ochiq holatga keltirish talab etiladi. Bu esa xakerlar, insayderlar yoki bulut provayderlari tomonidan ma’lumotlarning o‘qilish xavfini tug‘diradi.Ushbu muammoning yechimi sifatida Gomomorfik shifrlash texnologiyasi taklif etiladi. Ushbu usul ma’lumotlarni shifrdan yechmasdan turib ular ustida hisob-kitoblarni bajarish imkonini beradi. Natijada bulut serveri foydalanuvchi ma’lumotlarini ko‘rmagan holda qayta ishlashi mumkin.

Panjara nazariyasi va LWE muammosini modellashtirish

Tadqiqotda asosiy e’tibor Panjara nazariyasiga (Lattice-based cryptography)asoslangan sxemalarga qaratildi. FHE xavfsizligi "Learning With Errors" (LWE) matematik muammosining murakkabligiga asoslanadi. Biz quyidagi matematik modelni tahlil qildik:LWE muammosida shifrmatn quyidagi ko‘rinishda bo‘ladi:$c = a \cdot s + m + e \pmod q$Bu yerda:c –hosil bo‘lgan shifrmatn vektori;a –ochiq ma’lum (public) vektor;s –maxfiy kalit (secret key);m –shifrlanayotgan xabar (message);e–kichik qiymatli tasodifiy "shovqin" (error/noise). Ushbu "shovqin" (e) gomomorfik shifrlashning asosi bo‘lib, u xavfsizlikni ta’minlaydi, lekin har bir arifmetik amal(ayniqsa ko‘paytirish) bajarilganda kattalashib boradi.

Gomomorfik shifrlash avlodlari va evolyutsiyasi Tahlil shuni ko‘rsatdiki, FHE texnologiyasi rivojlanish bosqichiga ko‘ra 4 ta avlodga bo‘linadi va ularning har biri ma’lumotlar bazasi uchun turlicha samaradorlikka ega:

1-avlod (Gentry, 2009): Nazariy isbot. Amaliyotda qo‘llash imkonsiz darajada sekin edi (bitta bitni qayta ishlash uchun 30 daqiqa vaqt talab qilgan).

2-avlod (BGV, BFV): Leveled FHE (Darajali FHE) tushunchasi kiritildi. Bu sxemalar "Bootstrapping" jarayonini cheklash orqali butun sonlar ustidagi amallarni tezlashtirdi. Ma’lumotlar bazasidagi Exact Match(aniq qidiruv) va Aggregation(yig‘indi hisoblash) uchun eng mos keladigan avlod hisoblanadi.

3-avlod (GSW): Gentry-Sahai-Waters sxemasi. Matritsalarni ko‘paytirishga asoslangan bo‘lib, mantiqiy darvozalar (logical gates) bilan ishlashda qulay.

4-avlod (CKKS, TFHE): Hozirgi kunda eng ommabop yo‘nalish. CKKS sxemasi suzuvchi nuqtali sonlar (floating-point numbers) bilan ishlash imkonini beradi, bu esa shifrlangan ma’lumotlar ustida Sun’iy Intellekt modellarini o‘qitish imkonini yaratadi.

Ma’lumotlar hajmining kengayishi (Ciphertext Expansion) Eksperiment davomida aniqlangan yana bir jiddiy muammo —bu saqlash hajmining ortishidir. **AES-256:4** baytlik (int32) son shifrlanganda hajmi deyarli o‘zgarmaydi (padding hisobiga ~16 bayt).

BFV (FHE):4 baytlik son shifrlanganda uning hajmi 16 KB dan 32 KB gachayetishi mumkin. Bu shuni anglatadiki, ma’lumotlar bazasi hajmi o‘rtacha 2000-4000 barobarkattalashadi. Bu nafaqat diskdagi joyni, balki tarmoq (Network Bandwidth) o‘tkazuvchanligini ham band qiladi.

4. Ishlash tezligi (Latency Benchmark) SELECT SUM(salary)so‘rovi bo‘yicha olingan natijalar:

1.MySQL (Plaintext):0.002 soniya.

2.Paillier (PHE):0.08 soniya (Qabul qilsa bo‘ladigan natija).

3.BFV (FHE):2.4 soniya (Sezilarli kechikish).

4.TFHE (Fully Homomorphic with Bootstrapping):45 soniya (Real vaqt rejimi uchun yaroqsiz).

Ushbu tadqiqot ishida ma’lumotlar bazasi xavfsizligining inqilobiy yo‘nalishi — Gomomorfik shifrlash texnologiyasi kompleks tahlil qilindi. Olib borilgan nazariy va empirik o‘rganishlar natijasida quyidagi yakuniy xulosalar shakllantirildi:

1.Absolyut maxfiylik kafolati: Gomomorfik shifrlash ma’lumotlar maxfiyligini saqlagan holda funksionallikni yo‘qotmaslik imkonini beruvchi yagona kriptografik vositadir. U "Zero-Trust" konsepsiyasini to‘liq amalga oshiradi va tashkilotlarga o‘z ma’lumotlarini uchinchi tomon (Cloud) serverlarida xavfsiz saqlash imkonini beradi.

2.Qo‘llanilish sohasi chegaralanganligi: Gentry sxemasi nazariy jihatdan mukammal bo‘lsa-da, amaliyotda uning sekin ishlashi va katta xotira talab qilishi hozircha uni keng masshtabda joriy etishga to‘sqinlik qilmoqda. Hozirgi kunda FHE faqat yuqori darajadagi maxfiylik talab etiladigan kichik hajmdagi ma’lumotlar (masalan, biometrik shablonlar, DNK ketma-ketliklari, bank PIN kodlari) uchun maqbul yechimdir.

3.Gibrid yondashuv zarurati: Eng optimal yechim —bu gibrid arxitekturadir. Ya’ni, ma’lumotlarning 90% qismi an’anaviy (AES) usulda, faqat o‘ta maxfiy hisob-kitob talab qilinadigan 10% qismi Gomomorfik shifrlash yordamida himoyalanishi kerak.

4.Kelajak istiqbollari: Muammoning yechimi sifatida kelajakda faqat dasturiy optimallashtirish emas, balki maxsus apparat tezlatgichlari (Hardware Accelerators —FPGA, ASIC) ishlab chiqilishi kutilmoqda.

Foydalanilgan adabiyotlar.

1.Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University Doctoral Dissertation.

2.Acar, A., et al. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys,51(4), 1-38.

3.Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT).

4.Fan, J., & Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive.

5.Microsoft Research. (2023). Microsoft SEAL (Simple Encrypted Arithmetic Library) Manual. GitHub Repository.

6.Zokirov, S., & Karimov, A. (2022). Kriptografik usullar va ma'lumotlar himoyasi: Oliy o'quv yurtlari uchun darslik. Toshkent: "Fan va texnologiya".

7.Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM).

8.National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography Standardization Process.

LOKAL TARMOQLARDA DoS/DDoS HUJUMLARNI ERTA ANIQLASH ALGORITMI

Yusupov Behzod Ismoil o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universitetining Jiizzax filiali
Axborot tizimlari va texnologiyalari kafedrasi o'qituvchisi
Abduazimov Ravshan Azamat o'g'li, Elmurodov Xusan Ulug'bek o'g'li va Akaboyev Xolboy O'ralboy o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston
Milliy universitetining Jizzax filiali Amaliy matematika fakulteti
Axborot tizimlari va texnologiyalari yo'nalishi talabalari
ravshan200605@gmail.com

Annotatsiya. Ushbu maqolaning asosiy maqsadi lokal kompyuter tarmoqlarida yuzaga keladigan Denial-of-Service attack (DoS) va DDoS hujumlarini erta bosqichda aniqlash usullarini o'rganishdan iborat. Ishda tarmoq trafigidagi o'zgarishlarni tahlil qilish orqali anomaliyalarni aniqlashga asoslangan algoritm ishlab chiqish ko'zda tutilgan. Shuningdek, paketlar oqimi va trafik intensivligi asosida hujumlarni aniqlash mexanizmi taklif etiladi. Maqolada ishlab chiqilgan algoritmning amaliy jihatdan qo'llanilishi va samaradorligi ko'rib chiqiladi. Tadqiqot natijalari tarmoq xavfsizligini oshirish hamda xizmat uzilishlarini oldini olishga xizmat qiladi.